Privacy impact assessment and risk management

Report for the Information Commissioner's Office
prepared by Trilateral Research & Consulting
4 May 2013

This report was prepared by Trilateral Research & Consulting under a contract with the Information Commissioner's Office.[1] The work was done between mid-January 2013 and early May 2013 by the following:
David Wright, Managing Partner
Kush Wadhwa, Senior Partner
Monica Lagazio, Associate Partner
Charles Raab, Independent consultant
Eric Charikane, Independent consultant

A draft final report was submitted to the ICO on 28 March 2013 and the final report with recommendations was submitted on 4 May 2013.

For further information about Trilateral, please see www.trilateralresearch.com or e-mail: david.wright@trilateralresearch.com.

Copyright

[1] http://www.ico.gov.uk/about_us/research/data_protection.aspx

Contents

EXECUTIVE SUMMARY

Privacy impact assessments (PIAs) are widely used in the UK, especially by government departments and agencies, local authorities, national health service (NHS) trusts and even by companies, according to a survey carried out in early 2013, which found that more two-thirds of respondents were conducting privacy impact assessments.

The UK was the first country in Europe to develop and promulgate a privacy impact assessment methodology. The Information Commissioner's Office (ICO) published a PIA Handbook in December 2007, followed by a revision in June 2009.

The Cabinet Office accepted the value of PIA reports and stressed that they will be used and monitored in all departments as a means of protecting personal data from July 2008 onwards. PIAs have thus become a "mandatory minimum measure" in the UK government and its agencies.[2]

Following the ICO's lead, the European Commission introduced its proposed Data Protection Regulation in January 2012, Article 33 of which would make PIAs mandatory for both public and private sector organisations throughout Europe[3] where processing operations are likely to present specific risks to the rights and freedoms of data subjects.

While the ICO's PIA Handbook would appear to have had some success, the ICO has had concerns, which prompted the regulator to put out a tender in late 2012, the aim of which was

- To understand how privacy impact assessment (PIA) can be better integrated with existing project and risk management tools, and
- To help make PIA a more practical and effective tool.

Trilateral Research & Consulting won the tender. Work began on the present study was in mid-January 2013. Among other things, the study aims to provide input to the ICO, which intends to produce a further revision of its PIA guide in the coming months.

Methodology

Trilateral employed several different methodologies to determine to what extent PIAs are used in the UK, how they are used, comments by users on their efficacy, the extent to which they are integrated in project and risk management, how they could be better integrated, and recommendations for improving the PIA guidance.

First, we analysed the ICO's PIA Handbook and developed an analytical framework consisting of a two-column table with 16 "**touch points**". These touch points are key points or elements of the ICO PIA methodology. We converted these touch points into questions,

[2] See Cabinet Office, Cross Government Actions: Mandatory Minimum Measures, 2008, Section I, 4.4: All departments must "conduct privacy impact assessments so that they can be considered as part of the information risk aspects of Gateway Reviews". http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf. Gateway reviews are undertaken by an independent team of experienced people and carried out at key decision points in government programmes and projects to provide assurance that they can progress successfully to the next stage.

[3] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January 2012.

which we used throughout our study to interrogate other PIA methodologies, PIA reports, project and risk management methodologies. The aim was to locate similarities between these approaches and PIA that will provide opportunities for integration.

Second, for comparative purposes, we examined three other PIA frameworks.

Third, we compiled all of the publicly available UK PIA reports that we could find and analysed several of them using the "touch points".

Fourth, we sent out a questionnaire to 829 companies, central government departments and agencies, local authorities and NHS trusts, asking about their use of the ICO PIA Handbook and the extent to which they include privacy risks in their project and risk management practices.

Fifth, we conducted 12 in-depth case studies based on interviews with a mix of respondents to our survey and, in particular, from the private sector.

Sixth, we then analysed four project management methodologies and 15 risk management methodologies using our 16 touch points to see where we could find some commonalities. We also looked for "open doors", by which we mean any points in a project and/or risk management process where a PIA could be introduced.

Seventh, we conducted a "horizontal" analysis or comparative analysis of our findings, which eventually led us to the formulation of recommendations to the ICO.

The following pages summarise some of the key findings.

The PIA Handbook

The Handbook cautions that, because organisations vary greatly in size, the extent to which their activities intrude on privacy and their experience in dealing with privacy issues makes it difficult to write a "one size fits all" guide. Indeed, from the results of our survey and our analysis of existing PIA reports, the ICO was prescient – almost all organisations have adapted the guidance from the ICO Handbook according to their perceived needs.

According to the Handbook, a PIA is necessary for the following reasons: to identify and manage risks; to avoid unnecessary costs through privacy sensitivity; to avoid inadequate solutions to privacy risks; to avoid loss of trust and reputation; to inform the organisation's communication strategy and to meet or exceed legal requirements.

The PIA Handbook does well to emphasise that a PIA should not only consider personal data, but four different types of privacy, i.e., privacy of personal information, privacy of the person, privacy of personal behaviour and privacy of personal communication. Unlike Article 33 of the EC's proposed Data Protection Regulation, which is focused on only a data protection impact assessment, the Handbook ICO adopts a much wider view of privacy.[4]

Although other PIA guidance documents also mention these four types of privacy, the ICO Handbook provides more detail and clarity with regard to what is at stake. We strongly

[4] ICO, PIA Handbook, p. 14.

support the ICO's view of privacy as being more than just data protection. We think Article 33 is seriously deficient in reducing a "privacy impact assessment" to only a "data protection impact assessment". Organisations that carry out a DPIA may be fully compliant with data protection legislation, but could still intrude dangerously into an individual's privacy. Such a risk is greatly diminished if all types of privacy are considered, as the ICO Handbook rightly argues.

The Handbook foresees the utility of integrating PIA with risk management practices. It notes that "[r]isk management has considerably broader scope than privacy alone, so organisations may find it appropriate to plan a PIA within the context of risk management".

We distinguish between a PIA *process* and a PIA *report*. Engaging in a PIA is itself a valuable learning exercise for organisations, and some would argue that this process is more important than the report itself. The report is meant to document the PIA process, but in fact the PIA process extends beyond a PIA report. Even after the PIA assessor or team produce their report, which in most cases should contain recommendations, someone will need to make sure the recommendations are implemented or, if some are not, explain why they are not.

The PIA Handbook distinguishes between a full-scale PIA and a small-scale PIA. We think this is confusing for organisations. We do not think it is so easy to determine whether a full-scale or small-scale PIA is appropriate – despite (or perhaps even because of) the criteria in Appendix 1 of the Handbook. We suggest that, in a revised Handbook, the ICO simply say that PIAs are scalable, and that the scope, length and intensity of the PIA will depend on how serious the privacy risks are and on the numbers of people who might be impacted.

As a PIA methodology, the ICO Handbook has many good points. In revising it, or producing a third edition, the ICO should be careful not to throw the baby out with the bathwater. In view of comments made in interviews and other exchanges with organisations, our overall recommendation is that the methodology be streamlined. In a revised PIA Handbook, the ICO may wish to consider preparing a somewhat high-level, principles-based PIA methodology, perhaps with an annex of exemplary privacy risks and questions that could be used to uncover those risks. Sectors or organisations could then use this streamlined, principles-based guide for further development of a sector- or organisation-specific PIA attuned to the specificities of their sector or organisation.

Other PIA frameworks

Following our review of the PIA Handbook, for comparative purposes, we analysed three other PIA frameworks, namely, the RFID Framework which was endorsed by the Article 29 Data Protection Working Party in February 2011, Article 33 of the European Commission's proposed Data Protection Regulation, which would make PIA mandatory where organisations processing personal data present risks to data subjects, and the PIAF methodology which emerged from a project funded by the EC's Directorate General Justice and in which Trilateral was a partner.

Several data protection authorities said in their responses to the PIAF questionnaire that they preferred a streamlined, short, easy-to-understand and easy-to-use methodology. Hence, PIAF produced a six-page "Step-by-step guide to privacy impact assessment" and a six-page

"Template for a privacy impact assessment report".[5] We suggest that the ICO's third edition be like the "Step-by-step guide", but with two or three annexes identifying privacy risks, some questions aimed at uncovering those risks, and references to some particularly good risk assessment and risk management methodologies such as that of CNIL.

PIA reports

We then reviewed several publicly available PIA reports to see how well they track the guidance provide by the PIA Handbook. After a detailed search on the Internet, we identified 26 publicly available PIA reports in the UK, all of which bar two originate in the public sector. Of these, we selected several for more detailed analysis. Our interest in reviewing these PIA reports is to see how closely they track the ICO PIA Handbook, as represented by the 16 touch points. Further, our review of existing PIA reports helps to provide a view of how PIAs are currently practised by public and private organisations.

From our analysis of 26 publicly available UK PIA reports, we found that

- The majority of PIA reports number fewer than 30 pages.
- The number of publicly available PIA reports is growing (slowly).
- The vast majority of publicly available PIA reports have been produced by government departments and agencies; we found only two from industry.
- Among the various stated purposes for producing PIAs are concerns about privacy impacts, and impacts on the organisation's reputation.
- Most of the PIA reports acknowledge the ICO PIA Handbook; some say they have consulted the ICO for advice on the preparation of the PIA reports.
- Some PIA reports have said that they will be updated if there are any changes in the assessed project, programme or other activity involving the processing of data. Only one such update has been found on the Internet; it is not known whether PIAs have, in fact, been updated.
- Most PIA reports appear to have been produced "in-house"; only two of the 26 publicly available PIA reports were produced by external consultants, and those two were the only discovered PIAs that emanated from the private sector. While there is nothing wrong with using external consultants to conduct the PIA – some argue that using external consultants will give the resulting PIA reports more credibility – generally organisations need to build up their own internal PIA expertise.
- Almost all of the PIA reports examined for our study show that they were undertaken before their projects were finalised, when there was still an opportunity for the PIAs to influence the design or outcome of the project; this is good practice.

Surveys

Trilateral conducted three surveys germane to this study. The first, conducted in May 2012, was aimed at determining whether UK organisations are conducting PIAs and whether they experience fewer data breaches because they are, as a consequence of conducting PIAs, more careful with personal data.

[5] Both papers can be found here: http://www.piafproject.eu/Events.html

The second survey was in support of our tender proposal to the ICO, and was aimed at finding out which risk management methodologies UK organisations were using and whether respondents felt PIA could be integrated with their risk management practice.

The third, and much larger, survey was part of this study and expanded upon the first two surveys. Its purpose was to find out what percentage of responding organisations were conducting PIAs and how many they have conducted and whether PIA could be integrated in their project and risk management practices. For this survey, the questionnaire was distributed in January 2013 to 829 contact persons in central government bodies, NHS trusts, local authorities, and FTSE100 and FTSE250 companies.

The main findings from the surveys were that:

- More than two-thirds of responding organisations have done a PIA.

- Some organisations have done one, two or only a few PIAs, while others claimed that they have done vastly more.

- Respondents used a wide variety of project and risk management standards and methodologies. In the public sector, the Treasury's Orange Book was the main risk management guide and PRINCE2 was the most widely used project management methodology.

- All of the respondents consider, or are in the process of considering, privacy risk as part of their overall risk management process, and therefore focus on "the wide range of risks to which the project/activity is potentially exposed". All of the respondents have established close collaboration between the risk manager and the data protection officer regarding privacy risks, with the data protection officer working closely with the risk manager "on relevant issues, and providing updates to one another as to current guidance/awareness".

It was extremely difficult to compile contacts for private companies. Very little contact information is available on their websites. Switchboard and call centre staff were often unwilling to connect to named members of staff or provide e-mail addresses. There was little information about privacy and data protection processes on company websites, other than the generic website privacy policy. Where there was data protection information provided, there was no specified contact provided, and queries were directed towards the generic "info@..." e-mail address. In addition, even if the website provided the company's annual report, this did not include any specific names and/or contacts and was often difficult to find. As a result of the lack of publicly available contact information, we were forced to initially rely on company information, provided by stock market websites, and then on social networking sites as well as Trilateral's own network of professional contacts. Overall, the extent of information asymmetry that appears to characterise the relationship between the public and companies is striking.

Case studies

We undertook more than a dozen in-depth case studies, based on interviews conducted with selected respondents to the questionnaire. The case studies were of two types. The first type concerned PIA and its integration in the project and risk management practices of the

organisations. The second type concerned PIA and the policy-making process. We used the case studies to investigate more deeply how organisations have practically integrated PIA into their existing project and risk management methodologies and processes, as well as to identify key lessons learned from their experience of the integration and the use of the ICO PIA Handbook.

Among the highlights of the case studies are the following:

- Privacy is an important consideration for almost all of the organisations to whom we spoke. Many of them said privacy impacts were considered before or at the initiation of a project, e.g., at the procurement stage or formulation of a business case for a new project.

- To foster integration with project and risk management methodologies, more action needs to be taken. Several said it was important to gain buy-in from senior management and develop privacy awareness and culture within the company, sustained by effective communication and training. Organisations need to deliver a clear message to all project managers that the PIA process must be followed and that PIAs are an organisational requirement.

- Most said they adapted not only the PIA Handbook but also the project and risk management methodologies to meet their organisation's own, specific requirements.

- Most advocated a slimmed-down ICO Handbook and some said that the ICO should provide more practical tools and guidance on how to assess privacy risks, since organisations often do not have the knowledge and experience required to do so, and That the Handbook should more clearly indicate the benefits of PIAs.

From the various comments made by respondents in these case studies, the following are the key lessons that have helped to shape our recommendations:

- Ensuring the "buy-in" of the most senior people within the organisation is a necessary pre-condition for a successful integration of privacy risks and PIA into the organisation's existing processes. PIA processes need to be connected with the development of privacy awareness and culture within the company. Companies need to devise effective communication and training strategies to sustain a change in the mindsets of, and in the development of new skills for, project managers. The organisation needs to deliver a clear message to all project managers that the PIA process must be followed and that PIAs are an organisational requirement. Simplicity is the key to achieve full implementation and adoption of internal PIA guidelines and processes.
- An extensive and inclusive internal consultation, involving different parts of the organisation, is critical when defining the integration process. This will guarantee the full "buy-in" of all the interested and/or affected parties when the process is implemented.
- The documentation that the privacy team provides to support project managers when they do the PIA is important. Project managers must have all the information and the questions and answers they need to do a proper assessment. It is important to give them all the necessary data they need to allow them to make the necessary project adjustments in order to be fully compliant. Project managers need additional training and clear internal guidelines on how to do PIAs and complete PIA forms.
- All project plans should have a task on privacy, which will ensure that all of the privacy requirements are fully visible to and updated and monitored by project managers.

- Local authorities (indeed all organisations) need to establish central PIA repositories where all the PIAs conducted by the council are stored and can be accessed. This will promote a culture of sharing and benchmarking (i.e., councils can compare how well or badly they do in relation to privacy risks and PIAs), which in turn will support learning and self-improvement.

Project management standards and methodologies

Chapter 2 describes four popular project management standards and methodologies in use in the UK and abroad. These are:

- PMBOK
- PRINCE2
- Agile
- HERMES

For each methodology, we provide an overview followed by a table in which we "interrogate" the methodology using a set of questions derived from the PIA Handbook touch points. By developing a set of questions based on the PIA Handbook touch points to interrogate the project management methodology, we can determine whether there are sufficient commonalities between the PIA process and the project management process so that a PIA could be conducted in tandem with the project management process without disrupting it. Further, if there are a sufficient number of commonalities, then we assume that integration of PIA into the project management process will be possible without much difficulty. If there are an adequate number of touch points, we assume that it will be easier to convince project managers that they should take account of – or integrate – PIA in their project management process.

Even if there are not so many touch points, there is still a possibility of integrating PIA in the project management process through one or more "open doors" – i.e., points in the project management process where or when it would be possible to conduct a PIA.

The data collected from the January 2013 survey have been useful for identifying "open doors" that some of the surveyed organisations are already using in order to integrate privacy risks into their project management processes and adopted standards. Based on the responses, integration occurs, most of the time, at the project initiation phase, when the organisation needs to provide formal approval for, and finalise the scope and resources of the project. By taking the project life-cycle into consideration, we have identified possible open doors in three main phases: pre-project open doors, project-initiation open doors and project-implementation open doors.

Of the four PM methodologies reviewed, only one (HERMES) includes clear provisions for being compliant with a personal data protection law. By contrast, many of the risk methodologies say that organisations should comply with regulations; PIA does that, although it should also focus on risks that may not be covered by simple compliance with legislation. There is little emphasis in the project management methodologies on compliance.

Risk management standards and methodologies

Chapter 3 parallels the previous chapter to some extent. It describes 15 popular risk management standards and methodologies in use in the UK and abroad. The principal differences are that the risk management area is much more diverse in terms of available standards to be applied, and the scope of each differs. For each methodology, we provide an overview followed by a table in which we "interrogate" the methodology using the 16 touch points. We analysed the following:

- ISO 31000:2009 Risk management — Principles and guidelines
- Combined Code and Turnbull Guidance
- the Orange Book
- ENISA's approach to risk management
- ISO/IEC 27005:2011 Information security risk management
- IT-Grundschutz
- NIST SP 800-39 Managing Information Security Risk
- ISACA and COBIT
- CRAMM (Central Computer and Telecommunications Agency Risk Analysis and Management Method)
- EBIOS
- OCTAVE®
- NIST SP 800-30 Guide for Conducting Risk Assessments
- ISO/IEC 29100:2011 Information technology — Security techniques
- NIST SP 800-122, Guide to Protecting the Confidentiality of PII
- CNIL methodology for privacy risk management.

All of these methodologies and standards have at least some touch points in common with PIA. ISO 31000, ISO 27005, ENISA, EBIOS, NIST SP 800-122 and CNIL's approach have quite a few.

From the survey and case studies analysis, we could regard the integration of privacy risk and PIA into the risk management processes as a necessary pre-condition for achieving an effective integration of privacy risk and PIA into project management processes. Furthermore, virtually all methodologies offer "open doors", points at which it would be possible to conduct a PIA, in whole or in part. We identified two categories of open doors: at *the risk corporate level* and at *the single-risk project level*. The corporate level refers to the integration of privacy risks and PIA into overarching, macro-corporate frameworks, while the single risk-project level indicates operational integration at the micro, individual project level.

Horizontal analysis

A horizontal analysis of the various project and risk management methodologies identifies some commonalities and differences with regard to the "touch points"– i.e., points of commonality between the PIA process and the project and risk management methodologies – and the "open doors" – i.e., where a PIA could interface with the project or risk management methodology or when in the project or risk management process a PIA could be conducted in whole or in part. We found that:

- Although the dominant project management methodologies (PMBOK and PRINCE2) differ significantly, they share a structured, process-driven approach to managing projects towards specific, well-defined business objectives. This structured approach provides a good basis for integration of PIAs. In each case, the methodology does not include any specific focus upon the core issues of privacy and data protection, but rather, provides a framework within which these issues can be addressed.

- ISO 31000 appears to be the most prevalent risk management methodology. It shares some "touch points" with PIA, but because it is a generic risk management methodology, it does not address some PIA issues – for example, it does not use the word "privacy", not is there any provision that might suggest recognition of data protection risks. However, communication and consultation with stakeholders are integral to the risk management process, hence, there are some "open doors" in the process where a PIA could be conducted. There is nothing in the standard that would be at odds with a PIA.

- There is some comparability between PIA and the Turnbull guidance. There is nothing in the Turnbull guidance that would act as a barrier to including a PIA in a listed company's risk management process.

- Although the Orange Book does not focus on risks to individuals, many of the points in its risk-management methodology seem compatible with PIA, and the way it addresses risk through an analysis of preventive and corrective controls could also provide a gateway for considering privacy impact as part of a mitigating strategy. So, too, could the Orange Book's concern with stakeholder expectations. Its discussion of potential risks brought about by new projects could also provide an "open door" if such projects involved new IT projects and systems, for which the need for a PIA could be identified within a privacy risk management routine.

- The ENISA risk management methodology meets many of the PIA "touch points". It offers several "open doors" (or interfaces) for integration of its risk management methodology with other corporate operational processes. Also of interest is ENISA's distinction between existing and emerging risks, and its approach to each. It manages existing risks using a somewhat tried and tested (but traditional) risk management approach, whereas it uses relatively elaborate scenarios to explore emerging risks.

- ISO 27005 has many "touch points" in common with the PIA Handbook. There are also several "open doors" for PIA to be done:
  - during the environmental scan (context establishment) phase
  - as part of the risk identification process (common to both ISO 27005 and PIA)
  - during the process of identifying controls (counter-measures) against the risks in preparing the risk treatment plan. The most appropriate part would be in identifying risks and, subsequently, controls.

Further observations

Before giving our recommendations, some further observations can be made on the basis of the analysis in the report:

- While there are commonalities between the project and risk management processes and the PIA process, most of the methodologies do not mention privacy risks or even risks to the individual. Nevertheless, to the extent that privacy risks pose risks to the organisation, the organisation should take account of such risks in their project and risk management processes, including listing such risks in the organisation's risk register. It should not be too difficult to convince organisations of the importance of taking privacy risks into account and regarding privacy risk as another type of risk (just like environmental risks or currency risks or competitive risks). Especially in industries that deal directly with the general public – for example, banking, entertainment, and retail – privacy breaches, not confined to "data breaches", can be a significant threat to the company's reputation. Based on examples of privacy breaches, it should not be too difficult to convince organisations about the need to guard against reputational risk.

- Many of the risk management methodologies include provisions for taking into account information security (as distinct from privacy risks), and specifically with regard to confidentiality, integrity and availability of the information. Few go beyond this with the notable exception of ISO 29100, which specifically addresses privacy principles, IT Grundschutz and the CNIL methodology on privacy risk management. One can note that the privacy part of IT Grundschutz was written by the German DPA, and that the CNIL is the French DPA. Helpfully, both the privacy part of IT Grundschutz and the guides published by the CNIL include catalogues of privacy threat descriptions supplemented by the corresponding privacy controls.

- Some of the project and risk management methodologies call for consulting or engaging stakeholders, especially internally, but some (e.g., ISO 31000, ISO 27005) externally as well. PIA does the same. Some of the project and risk management methodologies (e.g., ISO 31000, ISO 27005) call for reviewing or understanding or taking into account the internal and external contexts. This is true of PIA too.

- Some of the project and risk management methodologies emphasise the importance of senior management support and commitment, which is also important for successful PIAs. Some of the risk management methodologies call for embedding risk awareness throughout the organisation. Some call for training staff and raising their awareness, which is also essential to PIAs.

- Almost all of the methodologies are silent on the issue of publishing the project or risk management report, although some do attach importance to documenting the process. Similarly, most are silent on the issue of independent, third-party review or audit to the project or risk management reports. There is, however, a requirement for companies listed on the London Stock Exchange to include information in their annual reports about the risks facing the company and how the company is addressing those risks.

Recommendations

The final chapter of our report provides recommendations on the practical steps the ICO can take to promote a better fit between PIA and project and risk management standards and

methodologies such as those described in this report. The recommendations are listed below, the detail of which can be found in Chapter 5.

Recommendations for the ICO

1. *We recommend that the ICO develop measures aimed at promoting a closer fit between PIA and risk- and project-management methodologies through direct contact with leading industry, trade, and other organisations in both the public and private sectors.*

2. *We recommend that, in revising its PIA Handbook, the ICO make the third edition much shorter, more streamlined, and more tailored to different organisational needs. It should be principles-based and focused on the PIA process. The ICO should undertake a consultation on a draft of a revised guidance document.*

3. *We recommend that the ICO's guidance on PIA emphasise the benefits to business and public-sector organisations in terms of public trust and confidence, and in terms of the improvement of internal privacy risk-management procedures and organisational structures.*

4. *We recommend that ICO guidance help organisations to understand and evaluate privacy risk, whether or not they can integrate PIA into their risk-management routines and methodologies.*

5. *We recommend that the ICO develop a set of benchmarks that organisations could use to test how well they are following the ICO PIA guidance and/or how well they integrate PIA with their project- and risk-management practices, especially where there are "touch points".*

6. We recommend that the ICO strongly urge PIA-performing organisations to report on how their PIAs have been implemented in subsequent practice, and to review the situation periodically.

7. *We recommend that the ICO promote to organisations the benefits of establishing repositories or registries of PIAs. We recommend that the ICO compile a registry of publicly available PIA reports, or at least a bibliography of such reports.*

8. *We recommend that the ICO take advantage of the current work within ISO to develop a PIA standard, and the BSI's technical panel's contribution to it.*

9. *We recommend that the ICO audit the PIA process and PIA reports in at least a sample of government departments and agencies*.

10. *We recommend that privacy risk be taken into explicit account in the Combined Code for companies listed on the London Stock Exchange.*

11. *We recommend that privacy risk be inserted into government guidance such as the Treasury Orange Book and the Green Book on appraisal and evaluation in central government.*

12. *We recommend that, at senior ministerial and official levels in government departments, and among special advisers, the ICO engage in dialogue to underline the importance of*

privacy and PIA while developing new policy and regulations and in the communication plans accompanying new policies.

13. *We recommend that the ICO encourage the Treasury to adopt a rule that PIAs must accompany any budgetary submissions for new policies, programmes and projects.*

14. *We recommend that the ICO encourage ENISA to support the ICO initiatives with regard to insert provisions relating to PIA in risk management standards as well as within ENISA's own approach to risk assessment.*

15. *We recommend that the ICO accelerate the development of privacy awareness through direct outreach to organisations responsible for the training and certification of project managers and risk managers.*

Recommendations for companies and other organisations

16. *We recommend that, to help embed PIA and to integrate it better with project and risk management practices, a requirement to conduct a PIA be included in business cases, at the inception of projects, and in procurement procedures. Organisations should require project managers to answer a simple PIA questionnaire at the beginning of a project or initiative to determine the specific kind of PIA that should be undertaken.*

17. *We recommend that senior management take privacy impacts into consideration as part of all decisions involving the collection, use and/or sharing of personal data.*

18. *We recommend that companies and other organisations review annually their PIA documents and processes, and should consider the revision or updating of their processes as a normal part of corporate performance management.*

19. *We recommend that companies and other organisations embed privacy awareness and develop a privacy culture, and should provide training to staff in order to develop such a culture. High priority should be given to developing ways of incorporating an enhanced PIA/risk assessment approach into training materials where information-processing activities pose risks to privacy and other values.*

20. *We recommend that companies and other organisations include contact details on their PIA cover sheets identifying those who prepared the PIA and how they can be contacted. The PIA should promote the provision of a contact person as "best practice". Such practice needs to be made mandatory certainly within any government organisation and any organisation doing business with the government. Such practice should also be promoted within standards organisations.*

21. *We recommend that public-sector organisations insert strong requirements in their procurement processes so that those seeking contracts to supply new information systems with potential risk to privacy demonstrate their use of an integrative approach to PIA, risk management and project management.*

22. *We recommend that companies and other organisations include privacy in their governance framework and processes in order to define clear responsibilities and a reporting structure for privacy risks.*

23. *We recommend that companies and other organisations include a PIA task, similar to a work-package or a sub-work-package, in their project plan structures in order to embed PIA better within project management practices, and that project managers monitor and implement this new privacy task, based on the identified privacy requirements, as is done in the case of other project tasks.*

24. *We recommend that, to foster internal buy-in for any newly adopted processes and procedures, companies and other organisations undertake extensive internal consultation with all parts of the organisation involved in risk management and project management, when thinking of integrating PIA into existing organisational processes.*

25. *We recommend that companies and other organisations include identified privacy risks in their corporate risk register, and that they update their register when new or specific types of privacy risk are identified by implementation teams.*

26. *We recommend that companies and other organisations develop practical and easy guidance on the techniques for assessing privacy risks and actions to mitigate them.*

1 INTRODUCTION

The Information Commissioner's Office (ICO) is currently considering how its privacy impact assessment (PIA) methodology and accompanying guidance material can be improved. The ICO has identified areas for potential improvement, one of which is better integration between PIAs and existing project management and risk management processes. Accordingly, in late 2012, it tendered for a research project, won by Trilateral, whose team comprised David Wright, Kush Wadhwa, Monica Lagazio and independent consultants Charles Raab and Eric Charikane, to look at PIAs and various project and risk management methodologies. The tender had two main requirements:

- To understand how PIA can be better integrated with existing project and risk management tools
- To help make PIA a more practical and effective tool.

1.1 PRIVACY IMPACT ASSESSMENT

The use of PIA in the UK dates back to at least December 2007, when the ICO published the first PIA Handbook in Europe.[6] The Handbook was based on research conducted by an internationally distinguished team led by Loughborough University. Among the PIA analysts in this team were Professor Colin Bennett (University of Victoria, B.C., Canada) and privacy and surveillance expert Roger Clarke, a consultant and Professor in Australia. The research team studied and produced reports on PIA practice and methodology in Australia, Canada, Hong Kong, New Zealand and the United States[7] in order to identify best practices that could inform the ICO Handbook, the principal author of which was Clarke. The ICO issued a second edition of the Handbook in June 2009.[8] It is now working on a third edition, and the Trilateral study is to provide some research upon which the new version can draw. We understand that the new PIA guidance will be somewhat shorter and more streamlined than its predecessors. Based on the present study as well as previous research conducted by Trilateral, especially in the context of the EC-funded PIAF project as well as our contacts with industry, we concur that a more streamlined guide is warranted.

Privacy impact assessments have been used since the 1990s.[9] Although there are differences between the PIA policies and methodologies in these countries, there is an increasing

[6] ICO, *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, UK, Version 1.0, December 2007.

[7] ICO, *Privacy Impact Assessments: International Study of their Application and Effects*, Information Commissioner's Office, Wilmslow, Cheshire, UK, December 2007. http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/privacy_impact_assessment_international_study.011007.pdf

[8] ICO, *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, UK, Version 2.0, June 2009 (hereafter ICO Handbook 2009). http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html.

[9] Among the early pioneers are Blair Stewart, the assistant privacy commissioner of New Zealand; Roger Clarke; Nigel Waters, formerly deputy privacy commissioner of Australia; Elizabeth Longworth, then a consultant in Australia and now a high-ranking official at the UN, and David Flaherty, former privacy commissioner of British Columbia. All these participated in a Privacy Issues Forum in Christchurch, New Zealand, in June 1996. Papers by Stewart and Longworth identify the parameters of the concept of PIA as it is understood today; see Stewart, Blair, "PIAs – an early warning system", *Privacy Law and Policy Reporter*, Vol. 3, No. 7, October/November 1996. http://www.austlii.edu.au/au/journals/PLPR/1996/65.html; Longworth, Elizabeth, "Notes on Privacy Impact Assessment", Longworth Associates, for Privacy Issues Forum, Christchurch, 13 June 1996; Stewart, Blair, "Privacy impact assessments", *Privacy Law and Policy Reporter*, Vol. 3, No. 4, July 1996. http://www.austlii.edu.au/au/journals/PLPR/1996/39.html. For more details about the origins of PIA, see Clarke, Roger, "Privacy Impact Assessment: Its Origins and Development", *Computer Law & Security Review*, Vol. 25,

convergence in approaches, in good part because later countries, such as the UK and Ireland, sought to learn from the experience of others. The increasing convergence is manifested by, for example, the emphasis on stakeholder consultation which features strongly in the UK and Irish PIA guidance documents, but less so or not at all in some of their antecedents. Convergence is also seen in definitions too, for example, of the term "project". Even certain phrases (PIA is described as "an early warning system") turn up again and again.

In terms of its influence alone, the UK PIA Handbook has been a considerable success. From the earliest days of the Handbook, the importance of PIA as an instrument for privacy protection has been well recognised. The Data Sharing Review Report recommended the use of PIAs.[10] The Cabinet Office, in its Data Handling Review, called for all central government departments to "introduce Privacy Impact Assessments, which ensure that privacy issues are factored into plans from the start".[11] It accepted the value of PIA reports and stressed that they will be used and monitored in all departments as a means of protecting personal data and tackling identity management challenges from July 2008 onwards. PIAs have thus become a "mandatory minimum measure" in the UK government and its agencies.[12]

Publication of the ICO PIA Handbook has undoubtedly been the most influential event in the subsequent promotion and promulgation of PIA in Europe. In May 2009, the European Commission issued its Recommendation on RFID, in which it called upon the Member States to provide inputs to the Article 29 Data Protection Working Party for development of a privacy impact assessment framework for the deployment of radio frequency identification (RFID) tags. In February 2011, the Article 29 Working Party endorsed an industry-developed PIA Framework for RFID.[13] The Commission then issued a mandate to the European Standards organisations CEN and ETSI to assess whether a translation of the PIA Framework into a standard would be feasible.[14]

The Commission also asked a Smart Grid Task Force (SGTF) to prepare a data protection impact assessment template for smart grid and smart metering systems.[15] Expert Group 2 of

---

No. 2, April 2009, pp. 123-135. PrePrint at http://www.rogerclarke.com/DV/PIAHist-08.html. In 1994, Tom Wright, the Ontario Information and Privacy Commissioner, called for organisations to prepare a "privacy impact statement" when introducing a potentially privacy-intrusive technology; see "Privacy Protection Makes Good Business Sense", Information and Privacy Commissioner, Toronto, 1994, Appendix D. http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=327.

[10] Thomas, Richard, and Mark Walport, *Data Sharing Review Report*, 11 July 2008. http://www.justice.gov.uk/reviews/docs/data-sharing-review-report.pdf; incorporated into CESG (the UK Government's National Technical Authority for Information Assurance), *HMG Information Assurance Standard No 6 – Protecting Personal Data and Managing Information Risk*. http://www.cesg.gsi.gov.uk/ia-policy-portfolio/hmg-ia-standards.shtml

[11] Cabinet Office, Data Handling Procedures in Government: Final Report, June 2008, p. 18. http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf

[12] See Cabinet Office, Cross Government Actions: Mandatory Minimum Measures, 2008, Section I, 4.4: All departments must "conduct privacy impact assessments so that they can be considered as part of the information risk aspects of Gateway Reviews". http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf. Gateway reviews are undertaken by an independent team of experienced people and carried out at key decision points in government programmes and projects to provide assurance that they can progress successfully to the next stage.

[13] For a description of the steps that led to the construction of the RFID PIA Framework, see Chapters 15 and 16 in Wright, David, and Paul De Hert, *Privacy Impact Assessment*, Springer, Dordrecht, 2012. This Framework is analysed in the present report.

[14] http://europa.eu/rapid/press-release_SPEECH-11-236_en.htm

[15] This template was submitted to the Article 29 Working Party for consultation according to the point 5 of the Recommendation on the roll out of smart metering systems. European Commission, Commission

the SGTF produced a first draft which was considered (and criticised) by the Art. 29 Working Party at its meeting at the end of January 2013.

Ireland's Health Information and Quality Authority followed the ICO approach in conducting an international study of PIA,[16] which led to the production of its PIA Guidance in December 2010.[17] Slovenia has produced a rudimentary PIA guidance document[18] and other countries in Europe are known to be developing PIA guides too, a process that may accelerate soon as a consequence of the proposed Data Protection Regulation. The European Commission includes a measure in its proposed Regulation that would make PIAs mandatory for any organisation.[19] Under Article 33, organisations would be obliged to conduct a "data protection impact assessment" where processing operations present specific risks to the rights and freedoms of data subjects.

Meanwhile, the International Organization for Standardization (ISO) has initiated the development of a standard for PIAs. It aims to complete its work by the time the proposed Regulation is adopted (2014 is the target) and comes into force two years later.

1.2 PIA AND RISK MANAGEMENT

The genesis of the contract awarded to Trilateral to study and recommend ways of improving integration of PIA in risk management might already be seen in the PIA Handbook. The ICO saw PIA as an element in risk management, as the Handbook makes clear. It says that "organisations may find it appropriate to plan a PIA within the context of risk management".[20] It also says that the government "will check that they have been carried out as an integral part of the risk management assessment".[21]

Better integration of PIA with risk management practices has been an issue with other data protection authorities, as the following paragraphs show, and for quite some time too. In one of the earliest papers on PIA, Elizabeth Longworth (1996) describes PIA as a risk management tool.

Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems, 2012/148/EU, Official Journal of the European Union L 73/9, 13.3.2012. Point 5 reads as follows: "In order to guarantee protection of personal data throughout the Union, Member States should adopt and apply the data protection impact assessment template to be developed by the Commission and submitted to the Working Party on the protection of individuals with regard to the processing of personal data for its opinion within 12 months of publication of this Recommendation in the Official Journal of the European Union."

[16] Health Information and Quality Authority, *International Review of Privacy Impact Assessments*, 2010. http://www.hiqa.ie/standards/information-governance/health-information-governance

[17] Health Information and Quality Authority, *Guidance on Privacy Impact Assessment in Health and Social Care*, Dublin, December 2010. http://www.hiqa.ie/resource-centre/professionals

[18] Information Commissioner RS, *Privacy Impact Assessment in e-Government Projects*, Information Commissioner's Guidelines, Slovenia, 22 July 2011.
https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/PIASmernice__ENG_Lektorirano_10._6._2011.pdf

[19] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January 2012.

[20] PIA Handbook, p. 5.

[21] PIA Handbook, p. 6. For a discussion of privacy protection and risk management, see Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, The MIT Press, Cambridge, MA, 2006, Chapter 3, and pp. 260-262, quoting White, F., "The Use of Privacy Impact Assessments in Canada", *Privacy Files*, Vol. 4, No. 7, 2001, pp. 1-11.

Australia's PIA Guide says: "PIA information feeds into broader project risk management processes."[22]

The PIA guide produced by the Office of the Victorian Privacy Commissioner (OVPC) says categorically that PIAs "should be an important part of the risk management and planning processes of all organisations".[23]

In its Directive on Privacy Impact Assessment promulgated in April 2010, the Treasury Board of Canada Secretariat states that "The PIA is the component of risk management that focuses on ensuring compliance with the Privacy Act requirements and assessing the privacy implications of new or substantially modified programs and activities involving personal information."[24] The Directive goes on to say that if a PIA is "not properly framed within an institution's broader risk management framework, conducting a PIA can be a resource-intensive exercise." Ontario's *Privacy Impact Assessment Guide* describes PIA as "both a due diligence exercise and a risk management tool".[25]

While these other PIA guides see PIA as part of the risk management process, one can ask: Has PIA, in fact, been successfully integrated into risk management processes? The best evidence so far seems to suggest that such integration remains more a wish than a reality. Following its major audit of government institutions' PIAs in 2007, the Office of the Privacy Commissioner in Canada (OPC) said in its report that "the PIA process was far from being fully integrated into the overall risk management strategies of individual entities". (PIAs are mandatory in the Canadian government.) In fact, the OPC found that "Privacy impact assessments were *rarely* integrated into the risk management strategies of organisations".[26] The Canadian Privacy Commissioner, Jennifer Stoddart, writes:

> In order to better encourage the early consideration of privacy risks, we believe there is a need to integrate PIA practices with an organisation's overall approach to risk management. This occurs not only at an operational level – that is, through the PIA triggers or screening devices previously discussed – but by linking existing regulatory requirements with other program activities and their administrative processes. Ideally, senior managers should be using privacy impact assessment, in conjunction with other social and economic analyses, to influence the subsequent development of programs, services, plans and policies. And where privacy impact assessment can be linked to a statutory requirement (irrespective of whether PIAs are made mandatory by law), there is a greater likelihood that they will be employed as a risk management tool prior to a program's deployment. While this is more likely to occur once an

[22] Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, Sydney, NSW, August 2006, revised May 2010, p. vii. http://www.privacy.gov.au. On 1 November 2010, the Office of the Privacy Commissioner was integrated into the Office of the Australian Information Commissioner (OAIC).

[23] Office of the Victorian Privacy Commissioner (OVPC), *Privacy Impact Assessments: A guide for the Victorian Public Sector*, Edition 2, April 2009, p. 2.
http://www.privacy.vic.gov.au/privacy/web2.nsf/pages/publication-types?opendocument&Subcategory=Guidelines&s=

[24] Treasury Board of Canada Secretariat, Directive on Privacy Impact Assessment, Ottawa, 1 Apr 2010, section 3.3. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=text

[25] Office of the Chief Information and Privacy Officer (OCIPO), *Privacy Impact Assessment Guide for the Ontario Public Service*, Queen's Printer for Ontario, December 2010, p. 6.

[26] Stoddart, Jennifer, "Auditing Privacy Impact Assessments: The Canadian Experience", Chapter 20, in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, pp. 419-436 [p. 430]; emphasis added. The OPC audited nine government departments and agencies and surveyed 47 others [pp. 424-425].

> organisation deems personal information and privacy as a strategic variable, its importance may be imposed through the integration of PIAs with other operational requirements.[27]

Stoddart makes several important points here, not least of which is her saying that PIAs are more likely to be used as a risk management tool where there is a statutory requirement to do so and that the integration of PIAs with other operational requirements may need to be imposed.

1.3 METHODOLOGIES

The research on which this report is based uses various approaches and methodologies.

We conducted a literature review of the various project and risk management standards and methodologies analysed in this report. An Internet search located 26 UK privacy impact assessment reports. Our analysis of these PIA reports is one of the few such attempts to comprehend the state of the art as practised in the UK.

We developed a short questionnaire of six questions, to make it as easy as possible to answer. Its purpose was to determine which project and risk management standards and methodologies are being used in the UK, whether the recipient organisations have conducted any PIAs (and if so, how many); whether PIA is integrated or could be integrated – according to the respondents – in their project and risk management practices; and whether the DPO and risk manager talked to each other.

Trilateral developed a list of data protection officers (DPOs) and risk managers from about 850 companies, UK central government departments and agencies, local authorities and NHS trusts, to whom we e-mailed the questionnaire directly. In addition, the ICO sent the questionnaire to about 1,300 people who applied to attend its annual DPO conference in March 2013. The ICO also included the questionnaire in the material handed out to participants on the day of the conference. Martin Hoskins, chairman of the Data Protection Forum, sent the questionnaire to its members with a covering letter. The International Association of Privacy Professionals (IAPP) ran an item about our study in its Europe Data Protection Digest, which it e-mailed on 25 January 2013 to about 4,900 members in Europe.

Trilateral also conducted a number of interviews with some of the respondents in our survey to go into deeper detail about their use of PIAs and the extent to which they are integrated with the organisation's project and risk management practices. Some of these interviews resulted in the case studies in Annex 3 of this report. A few other interviews were conducted by Trilateral to gather additional information about some of the project management methodologies.[28]

The ICO allowed Trilateral team members to attend the DPO conference in Manchester on 5 March 2013, providing an opportunity to meet other participants. David Wright, Trilateral's managing partner, gave a presentation about our study, together with the ICO project officer, Tom Oppé, in three different sessions during the conference. In two of these sessions, the audience were asked for a show of hands to indicate who had conducted a PIA or worked in an organisation that had conducted one. About a third or more had done so; this is in line with the findings of our survey. PIAs appear to be widely used by many organisations in the UK.

[27] Stoddart, ibid., p. 430.
[28] We thank all those whom we interviewed for giving generously of their time.

By contrast, a survey was conducted of data protection authorities in Europe to determine how many RFID PIAs they had reviewed or of which they were aware; the response from all DPAs was nil. We believe PIAs are more widely conducted in the UK, in part because they are mandatory in central government, but not only for this reason. We know that some companies are conducting PIAs, especially because they value their reputation and wish to earn the trust of customers, and because they do not want to compromise their customers' personal data, which might damage their reputation.[29]

For this study, Trilateral developed an analytical framework which consisted of a two-column table with 16 "**touch points**" drawn from the ICO PIA Handbook. These touch points were key points or elements of the ICO PIA methodology. We converted these touch points into questions which we used to interrogate the PIA reports, the project and risk management standards and methodologies that we analysed for this study, and that are reported in Chapters 2 and 3. We then performed a "horizontal analysis" (a comparative analysis) of the results of each the project and risk management methodologies, which is reflected in Chapter 4 of this report.

Another term used in this study is "open doors", by which is meant any points in a project and/or risk management process where a PIA could be inserted and carried out.

1.4 STRUCTURE AND SCOPE OF THIS REPORT

This report comprises five chapters, seven annexes and an executive summary.

Following Chapter 1, this Introduction, Chapter 2 focuses on project management methodologies, for which PMBOK, PRINCE2, Agile and HERMES were reviewed, summarised and analysed. In each case, we conclude with a table showing our touch points and evidence of the extent to which the methodologies have similar features.

Chapter 3 focuses on 15 different risk management standards and methodologies, divided into four categories covering risk management, information security, risk analysis and privacy risk management. This chapter concludes with a section on practical approaches for integrating privacy risks into risk management methodologies and standards. The analysis of risk management standards and methodologies includes those in use in the public and private sectors. It also covers some methodologies (e.g., those of NIST, EBIOS and CNIL) that are important and well regarded internationally, but for which we found no evidence of their use in the UK. Nevertheless, we have included an analysis of a few such methodologies because they are of interest for comparing with those in use in the UK: Do they show any significant differences from those in use in the UK? Is there anything that we, in the UK, can learn from other methodologies used abroad? But most important, for present purposes, we wanted to see whether PIA can be integrated with these other approaches used outside the UK.

Chapter 4 contains the main findings of our study. It also provides a horizontal analysis (or comparative analysis) of the various parts of our study.

[29] See, for example, the chapters on Nokia, Siemens and Vodafone in Wright, David, and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012. For a discussion of the relationship between privacy and trust, see Bennett, Colin J. and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, The MIT Press, Cambridge, MA, 2006, pp. 49-57; 6, Perri, with Kristen Lasky and Adrian Fletcher, *The Future of Privacy, Volume 2: Pubic Trust in the Use of Private Information*, Demos, London, 1998.

Chapter 5 contains our recommendations.

Annex 1 is on PIA practices. It reviews the ICO PIA Handbook and identifies some of its key features which are the basis for the "touch points" we use to interrogate PIA reports and project and risk management methodologies. We also examine three other PIA approaches: the RFID PIA Framework, Article 33 of the proposed Data Protection Regulation and the PIAF methodology to see how they compare to the PIA Handbook touch points. We then examine seven PIA reports from the 26 listed in Annex 6.

Annex 2 summarises the results of the survey conducted especially for this study. We compare the results of this survey with two other, smaller surveys conducted by Trilateral in November 2012 and in May 2012. In addition to providing a view of how widely used PIAs are and how many have been conducted, the survey initiated in January 2013 helped us to identify those project and risk management approaches most widely used by respondents.

Annex 3 comprises case studies undertaken for this study, based on interviews with respondents. Although the ICO did not ask Trilateral to conduct such case studies, we felt they were useful in giving some deeper insights into the use of PIAs and their integration with project and risk management as well as how PIAs fit in with the policy-making process.

In Annex 4, we have reproduced the questionnaire used in this study. Annex 5 is a list of anonymised responses to the survey, showing how many PIAs each respondent has carried out. Annex 6 lists the publicly available UK PIA reports which we were able to discover after some hours of searching on the Internet. Annex 7 summarises the copyright situation regarding the various PIA, project and risk management documents on which we have drawn for preparation of this report.

In addition, there are two sets of references. The first provides the citations for the various project and risk management standards included in this study. The second is a list of the Trilateral team's various PIA publications for those who might want some further reading.

2 PROJECT AND TECHNOLOGY DEVELOPMENT MANAGEMENT STANDARDS AND METHODOLOGIES

This chapter describes popular project management standards and methodologies in use in the UK and abroad. For each methodology, we provide an overview followed by a table in which we "interrogate" the methodology using a set of questions derived from the PIA Handbook touch points (see Annex 1). The following table shows how we have converted the touch points into a set of questions.

	Touch points extracted from the ICO PIA Handbook	Questions for project management methodology based on touch points
1	PIAs must comply with (more than just data protection) legislation. Private sector organisations will also have to consider industry standards, codes of conduct and privacy policy statements.	Does the PM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?
2	PIA is a process.	Is the PM methodology regarded as a process or is it simply about producing a report?
3	A PIA could consider: 1. privacy of personal information; 2. privacy of the person; 3. privacy of personal behaviour; and 4. privacy of personal communications.	Does the PM methodology address only information privacy protection or does it address other types of privacy as well?
4	PIA should be undertaken when it is possible to influence the development of a project.	Does the PM methodology say that it should be undertaken when it is still possible to influence the development of the project?
5	Responsibility for the PIA should rest at the senior executive level.	Does the PM methodology place responsibility for its use at the senior executive level?
6	The organisation should develop a plan for the PIA and its terms of reference. It should develop a consultation strategy appropriate to the scale, scope and nature of the project.	Does the PM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?
7	A PIA should include an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources).	Does the PM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?
8	The organisation should determine whether a small-scale or full-scale PIA is needed.	Does the PM methodology include provisions for scaling its application according to the scope of the project?
9	A PIA should seek out and engage stakeholders internal and external to the organisation. The assessor needs to make sure that there is sufficient diversity among those groups or individuals being consulted, to ensure that all relevant perspectives are	Does the PM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?

	Touch points extracted from the ICO PIA Handbook	Questions for project management methodology based on touch points
	represented, and all relevant information is gathered.	
10	The organisation should put in place measures to achieve clear communications between senior management, the project team and representatives of, and advocates for, the various stakeholders.	Does the PM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?
11	The PIA should identify risks to individuals and to the organisation.	Does the PM methodology call for identification of risks to individuals and to the organisation?
12	The organisation should identify less privacy-invasive alternatives. It should identify ways of avoiding or minimising the impacts on privacy or, where negative impacts are unavoidable, clarify the business need that justifies them.	Does the PM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?
13	The organisation should document the PIA process and publish a report of its outcomes.	Does the PM methodology include provisions for documenting the process?
14	A PIA report should be written with the expectation that it will be published, or at least be widely distributed. The report should be provided to the various parties involved in the consultation. If information collected during the PIA process is commercially or security sensitive, it could be redacted or placed in confidential appendices, if justifiable.	Does the PM methodology include provision for making the resulting document public (whether redacted or otherwise)?
15	The PIA should be re-visited in each new project phase.	Does the PM methodology call for a review if there are any changes in the project?
16	A PIA should be subject to third-party review and audit, to ensure the organisation implements the PIA recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations.	Does the PM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?

By developing a set of questions based on the PIA Handbook touch points to interrogate the project management methodology, we can determine whether there are sufficient commonalities between the PIA process and the project management process so that a PIA could be conducted in tandem with the project management process without disrupting it. Further, if there are a sufficient number of commonalities, then we assume that integration of PIA into the project management process will be possible without much difficulty. If there are an adequate number of touch points, we assume that it will be easier to convince project

managers that they should take account of – or integrate – PIA in their project management process.

Even if there are not so many touch points, there is still a possibility of integrating PIA in the project management process through one or more "open doors" – i.e., points in the project management process where or when it would be possible to conduct a PIA.

2.1 PROJECT MANAGEMENT METHODOLOGIES

While project management methodologies continually evolve, and a small proportion of organisations (4%, according to the PWC 2012 global survey of companies[30]) use an in-house developed methodology, there are a few dominant (and emerging in dominance) project management approaches, which we describe here.

2.1.1 Project Management Body of Knowledge (PMBOK©)

With its origins as a white paper[31], and later expanded as the PMI (Project Management Institute) Project Management Body of Knowledge in the PMI-published *PM Network* periodical in 1987, this standard was approved as an ANSI (American National Standards Institute) standard in 1999.[32] On a global basis, 41 per cent of organisations responding to a survey by PriceWaterhouseCoopers report that PMBOK is the dominant project management methodology used globally[33] for managing all types of projects. As an indicator of the broad scope of adoption, PMI reports[34] that more than 650,000 people in 185 countries are members of PMI and credential holders in one of the areas related to PMBOK.

This standard encompasses a broad range of principles, process groups and knowledge areas for project management. The processes and knowledge developed and described under this standard have been written about and amended over several iterations by PMI volunteers, who have brought expertise from their work in the project management profession. The *PMBOK© Guide* acknowledges as well the "plan-do-check-act" cycle, as originally defined by Shewhart in the 1930s and further modified by Deming in the 1950s,[35] as an underlying concept for the interaction amongst these processes.

[30] PriceWaterhouseCoopers, *Insights and Trends: Current Portfolio, Programme, and Project Management Practice*. The third global survey on the current state of project management took place in 2012. See http://www.pwc.com/us/en/public-sector/publications/global-pm-report-2012.jhtml

[31] Ethics, Standards and Accreditation Report, PMI, 1983.

[32] Currently, ANSI Standard number ANSI/PMI 99/001/2008 corresponds to the 4th edition of the PMBOK Guide.

[33] PriceWaterhuseCoopers, op cit.

[34] http://www.pmi.org

[35] American Society for Quality, *ASQ Handbook*, 1999, pp. 13-14.

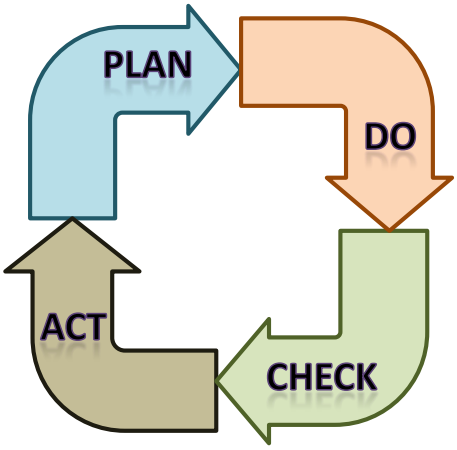


Figure 2.1: Plan-Do-Check-Act Cycle

The process groups (many of which are directly paralleled in ISO 21500,[36] the development to which PMI contributed) include those described below.

- *initiating* processes, which are associated with the initial definition or authorisation of projects or project phases,
- *planning* processes, which aim to define and/or refine goals and objectives and plan actions needed to achieve them,
- *executing* processes, where people and resources are brought together to complete the work that has been planned,
- *monitoring and controlling* processes, which are focused upon measuring and checking progress against the developed plan, and
- *closing* processes, that end the project or project phase in an orderly fashion, with a focus upon acceptance of the work performed.

Nine knowledge areas of PMBOK are required for project managers and applied (to a greater or lesser degree) across the five process groups described above. The knowledge areas defined and described in the standard include:

- Project Integration Management. This knowledge area focuses upon the integration of processes amongst the project management process groups. Within this knowledge area are described the development of the project charter, preliminary project scope and the overall project management plan.

- Project Scope Management. This knowledge area includes processes that aim to define the work of the project and ensure it encompasses all (but only) the work required to complete the project, as well as to control the scope over the course of the project through an integrated change control process. The scope of work is defined through a work breakdown structure (WBS) that deconstructs the work and identifies deliverables.

[36] The process groups for ISO 21500 are essentially the same as for PMBOK, with only a change in the names, which are initiating, planning, implementing (rather than executing), controlling (rather than monitoring and controlling), and closing. The parallels to the knowledge areas for ISO 21500 are integration, stakeholders (which is covered within communications under PMBOK), scope, time, cost, quality, resources (which encompasses both human and other types of resources), communications, risk and procurement.

- Project Time Management. This knowledge area comprises processes aimed at developing and managing the overall project schedule, including activity definition and sequencing, estimating resource and activity duration, and analysis required to develop a schedule from these inputs.

- Project Cost Management. This knowledge area includes those processes that support planning, estimating and controlling project costs. The over-arching aim served by these processes is to develop the project within its budget. This knowledge area includes concepts of life-cycle costing, along with value engineering techniques to improve decision-making within the project's life in order to optimise quality and performance.

- Project Quality Management. This knowledge area includes those processes that provide for the implementation of quality policies, objectives and responsibilities, implementing the quality system utilised by the organisation, and specifically organises this through quality planning, quality assurance and quality control activities. The standard describes and defines approaches to implement various quality standards and to monitor results to ensure they meet the quality standards. It provides for continuous improvement through the application of a cyclical "plan-do-check-act" cycle or other quality improvement initiatives (e.g., TQM, Six Sigma).

- Project Human Resource Management. This knowledge area includes processes often referred to as "soft skills". The processes include those aimed at organising and managing the project team, from human resource planning, defining roles and responsibilities, and staff management planning to acquiring, developing and managing the project team. The processes include quantitative planning efforts as well as guidance for negotiating for resources, team building, conducting performance appraisals and other soft management skills.

- Project Communications Management. This knowledge area comprises processes to link people and information within the project in order to ensure success of the project. Of the various principles and processes included in this knowledge area, managing stakeholders is of particular interest. The standard includes discussion of positive and negative stakeholders to highlight the need to understand the perspectives of each, though the general focus of the processes is upon the users whose inputs are directly sought to identify issues and initiate change requests.

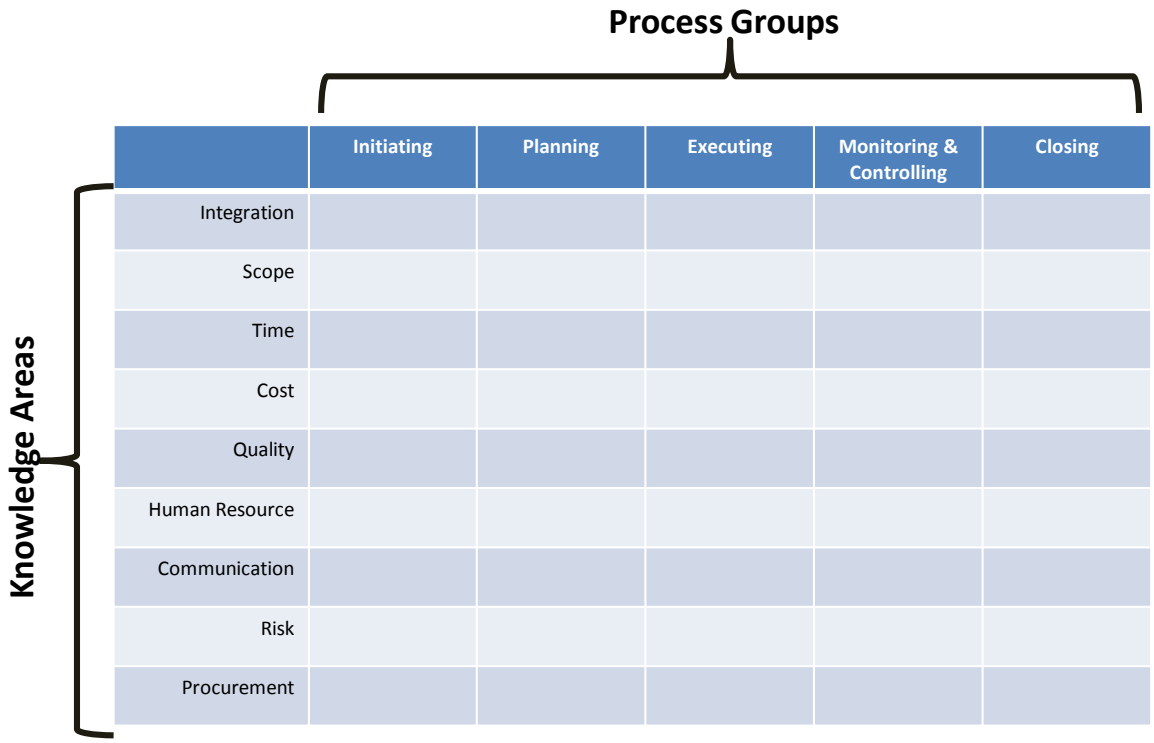


Figure 2.2: Process Groups and Knowledge Areas

- Project Risk Management. The processes included in the knowledge area are those connected to planning for, identification of, responding to, monitoring and controlling risk within a project. Risks are qualitatively and quantitatively analysed, and risk probabilities and impacts defined. A risk breakdown structure (RBS) is defined as an output of these processes. Given the uncertain nature of risk, numerous strategies for identifying and controlling risks are described.

- Project Procurement Management. This knowledge area includes the processes for acquiring or purchasing the products or services needed from sellers outside the project team, and includes activities for planning purchases and acquisitions and contracting, selecting sellers, performing contract administration and ultimately closing out contracts.

The methodology provides detailed, structured approaches to address each of the process areas within the context of each knowledge area, detailing steps to be completed and documents to be produced. In addition to the PMBOK© Guide, specific separate practice standards are provided for specific tools, techniques or processes identified in the PMBOK© Guide, including those for Project Risk Management, Earned Value Management, Project Configuration Management, Work Breakdown Structures, Scheduling, and Project Estimating. In addition, foundational standards are provided for construction projects and government-based projects as extensions of PMBOK©.

Of the nine knowledge areas, several should be particularly noted as they may apply to the integration of PIA:

- Project Integration Management. As this knowledge area focuses upon the integration of processes, and privacy impact assessments may be viewed as looking across the entirety of a project, introduction of privacy and data protection goals may be determined to be relevant within the project charter and/or scope.

- Project Scope Management. Specific goals for privacy and the conduct of a privacy impact assessment (or a cyclical implementation of privacy impact assessments over the course of multiple project phases) could be introduced in the scope of the project as developed and managed in this knowledge area.

- Project Communications Management. Specific processes for engaging stakeholders in the project as it relates to privacy impact assessment goals should be addressed through the communication management knowledge area.

- Project Risk Management. Privacy and data protection related risks are assessed via the PIA. This knowledge area would be appropriate for introducing and defining the tools and techniques associated with project risk management.

The documents which are produced by the project management professional, and are the focus of the PMBOK© Guide, are the Project Charter (formally authorising the project), the Project Scope Statement (stating the work to be done and deliverables expected), and the Project Management Plan (indicating *how* the work will be done).

The PMP accreditation associated with PMBOK© is the most widely held certification for project managers on a global basis. The certification is issued by the Project Management Institute (PMI), which also publishes the related standards as *A Guide to the Project Management Body of Knowledge (PMBOK© Guide)*, currently in its 5th edition (2013).

	Questions for project management methodology based on touch points	**Evidence from PMBOK© methodology**
1	Does the PM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	The PMBOK© Guide does not specifically provide for processes to assure compliance with regulatory or other issues, but does identify the need to incorporate such provisions in the process of developing the project charter as a determinant of project success.
2	Is the PM methodology regarded as a process or is it simply about producing a report?	The methodology is a process-driven approach, which is flexibly applied across all types and phases of projects.
3	Does the PM methodology address only information privacy protection or does it address other types of privacy as well?	There is no explicit focus upon privacy.
4	Does the PM methodology say that it should be undertaken when it is still possible to influence the development of the project?	This is not addressed by the methodology.
5	Does the PM methodology place responsibility for its use at the senior	The methodology encourages the inclusion of various types of

	Questions for project management methodology based on touch points	Evidence from PMBOK© methodology
	executive level?	stakeholders, including executive levels of management, particularly when initiating the project and gaining authorisation as well as in scope definition and acceptance.
6	Does the PM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	The methodology is heavily reliant upon developing a detailed plan, engaging stakeholders, and ensuring effective communication across the project.
7	Does the PM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	There is no explicit focus upon performing an environmental scan; however, as a part of the risk management aspects, identification of risk would include a risk assessment and probability analysis that would include lessons learned from other projects and sources.
8	Does the PM methodology include provisions for scaling its application according to the scope of the project?	This is not addressed by the methodology.
9	Does the PM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	There is a particular focus within the context of the Project Communications Management knowledge area on managing stakeholders and managing change to the project scope within that context.
10	Does the PM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	Yes. The Project Communications Management knowledge area addresses the principles and processes appropriate for clear communications amongst these groups.
11	Does the PM methodology call for identification of risks to individuals and to the organisation?	Yes, the Project Risk Management knowledge area addresses the identification of risks. Broadly, this looks at all types of risks to the project and its goals, but also at risks that may emerge from a wide range of sources (technical, environmental, etc.).
12	Does the PM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	The methodology does not explicitly aim to look for negative impacts of the project, but it is expected that both positive and negative stakeholders to the project should be engaged within the processes. That is, those stakeholders who are concerned about negative impacts will be expected to identify areas of concern.

	Questions for project management methodology based on touch points	Evidence from PMBOK© methodology
13	Does the PM methodology include provisions for documenting the process?	This methodology is heavily reliant upon developing written deliverables that define and describe the plan and the outcomes of the work performed.
14	Does the PM methodology include provision for making the resulting document public (whether redacted or otherwise)?	There is no provision for making documents public. Such standards would need to be defined at an organisational level.
15	Does the PM methodology call for a review if there are any changes in the project?	As there is no explicit call for PIA within the methodology, there is likewise no call for a review. However, the processes recognise the cyclical nature of a project with an integrated change control process, which may include its own criteria for initiation of a review of privacy issues based upon the nature of changes.
16	Does the PM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	No, there is no provision for audit of changes prescribed by a PIA within the methodology, but it may be that the change control process should include provisions for such follow-on validation.

Conclusions and recommendations

Privacy impact assessments have well-defined goals and can be very effectively integrated within the PMBOK framework. The main focal point for integration should be within the Project Risk Management knowledge area, and the PIA should be presented as an available tool for assessment of privacy risk (specifically, as a tool for activity 11.2). In addition, privacy and data protection should be introduced, along with regulatory and legislative factors as an environmental consideration when developing the project charter and scope, and in the context of change control.

2.1.2 PRINCE2 (PRojects IN Controlled Environments)

PRINCE2 (Projects in a Controlled Environment), originally published in 1996, is a project management standard developed by the UK Office of Government Commerce (OGC) and used widely within the UK government, alongside other OGC-developed methods and guidance. "PRINCE2 is a *de facto* standard developed and used extensively by the UK government and is widely recognised and used in the private sector, both in the UK and internationally. It embodies established and proven best practice in project management."[37]

This standard has evolved from earlier project management methods adopted by the Central Computer and Telecommunications Agency (CCTA), which was renamed to the Office of

[37] http://www.prince-officialsite.com/home

Government Commerce. The earlier incarnations of these methods included PRINCE, which was published in 1989, which had itself superseded PROMPT, a method dating to 1975, which had been adopted by the CCTA in 1979.

Beyond the broad use of the method within UK government organisations and agencies, this standard has been adopted on the global stage (most heavily in Australia and Europe where adoption is 20 per cent or greater[38]) and in both public and private sector organisations. PRINCE2 provides a structured framework for project management and, in practice, is complemented by the project management "soft skills" involved in managing projects.

The PRINCE2 framework integrates principles, themes, processes, and the project environment to enable a scalable, tailored approach to project management.[39]

Principles

The principles serving as a foundation for PRINCE2 are:

- Continued business justification. This justification is documented in a PRINCE2 setting in a business case.
- Learn from experience. Project teams operating in a PRINCE2 setting will review prior projects for lessons learned, or seek external inputs to help guide the project. This process of learning continues through the life of the project.
- Defined roles and responsibilities. The project team will include at least three primary stakeholders (refer to Figure 2.3), including business sponsors, users and suppliers, and the project structure will reflect the involvement and provide for engagement of each, with defined roles.
- Manage by stages. Projects in PRINCE2 have a minimum of two stages, including an initiation stage and one or more further management stages.
- Manage by exception. Tolerances are defined across time, cost, quality, scope, risk and benefit objectives, and where tolerances are exceeded, they are escalated to the next management layer for decision-making.

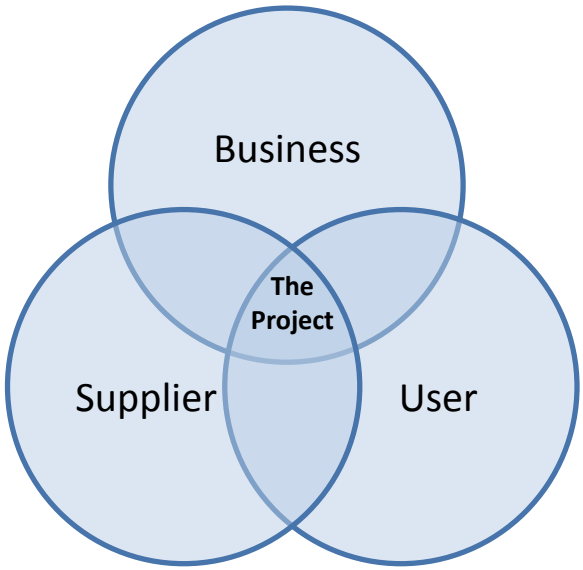


Figure 2.3: Project interests and stakeholders

[38] PriceWaterhouseCoopers, op cit.
[39] Office of Government Commerce, *Managing Successful Projects with PRINCE2™*, UK, 2009.

- Focus on products. PRINCE2 projects use a Product Description to provide clarity as to the purpose of the project, and the focus on product(s) of the project is aimed at fulfilling stakeholder expectations and is based upon business justification.
- Tailor to suit the project environment. PRINCE2 can be scaled in ways that will universally apply to different project environments, and whose project controls can adjust on the basis of scale, complexity, importance, risk or other factors.

Themes

PRINCE2 themes are aspects of project management that run throughout a project and are addressed on a continual basis. For each of the themes, PRINCE2 addresses how each aspect of project management is to be treated in order to ensure the processes (below) are as effective as possible. In addition, the themes for PRINCE2 provide a definition of responsibilities of each defined role within the theme.

- Business case. The business case is developed at the beginning of the project, verified and maintained throughout the course of the project's duration, and continuously confirmed that the intended benefits outlined in the business case are being realised. For example, the business case is developed during the pre-project and initiation stages, verified and benefits confirmed in each subsequent delivery stage, and benefits confirmed again at the final delivery and post-project stages. The business case would be expected to include the reasons for the project, its benefits and dis-benefits, timeline, cost, identification of major risks, and an appraisal of the investment (net benefits, ROI, payback period, or similar metrics). This continual re-evaluation of the business case provides an opportunity to ensure than business objectives, costs, timelines, benefits and risks remain in alignment.
- Organisation. PRINCE2 approaches a project as a temporary organisation aimed at delivering products based upon the developed and confirmed business case. The method introduces four levels of management, including three within the project management structure (directing, at the level of the project board; managing, at the level of the project manager; delivering, at the level of the team manager) and one level outside the project, which is at the corporate or programme management level. In this theme, guidance is provided on engaging stakeholders, whether internal or external to the project or organisation.
- Quality. The quality theme is tightly linked with the product focus principle, aimed at ensuring that the results of the project meet the expectations of the business and enable the expected benefits to be achieved. This theme focuses upon quality planning (i.e., establishing quality criteria, defining quality tolerance levels, defining quality methods, and assigning quality responsibilities) and quality control methods (testing, inspections). Structured inspections are used as an opportunity to engage with stakeholders along the duration of the project. Records are maintained to assure the completeness and adherence to quality criteria and that the products are accepted by stakeholders.
- Plans. This theme introduces a comprehensive approach to planning which includes a recommendation for three levels of plan, corresponding to the different levels of management (project, stage, team). The planning theme includes attention to various steps in developing plans, including designing the plan, defining and analysing products, identification of activities and dependencies, preparation of estimates and schedules, analysis of risk, and documentation of the plan, all of which are repeated for the overall project, individual stages and optionally for team plans.

- Risk. The PRINCE2 risk management approach is based upon the OGC's published guidance: *Management of Risk: Guidance for Practitioners* (TSO, 2010). M_o_R® principles, in turn, are informed by ISO31000:2009 (refer to section 3.1.1 for a discussion of ISO31000:2009) as well as corporate governance principles. M_o_R is examined in detail later in this section.
- Change. PRINCE2 addresses change control as a systematic, continual activity within the life of a project, and similarly addresses issues that arise that require management attention. It defines priority, severity and change authority. The change theme describes the approach to change which include controls for a configuration management strategy, as well as records that describe configuration items and their status. It also outlines a configuration management procedure to include steps for capturing, examining, proposing, deciding, and implementing change.
- Progress. This theme focuses upon the mechanisms required to monitor progress within the project against the objectives of the plan, established tolerances, and ensure effective escalation when required. Progress control is provided through delegation of authority, division into managing stages, event- and time-driven reviews and reporting, as well as raising of exceptions. The progress theme also ties into the organisation theme, delegating definition of tolerances and exception reporting across the four levels (corporate or programme management, project board, project manager, team manager).

Processes

The seven processes of PRINCE2 provide the specific activities for directing, managing and delivering a project.

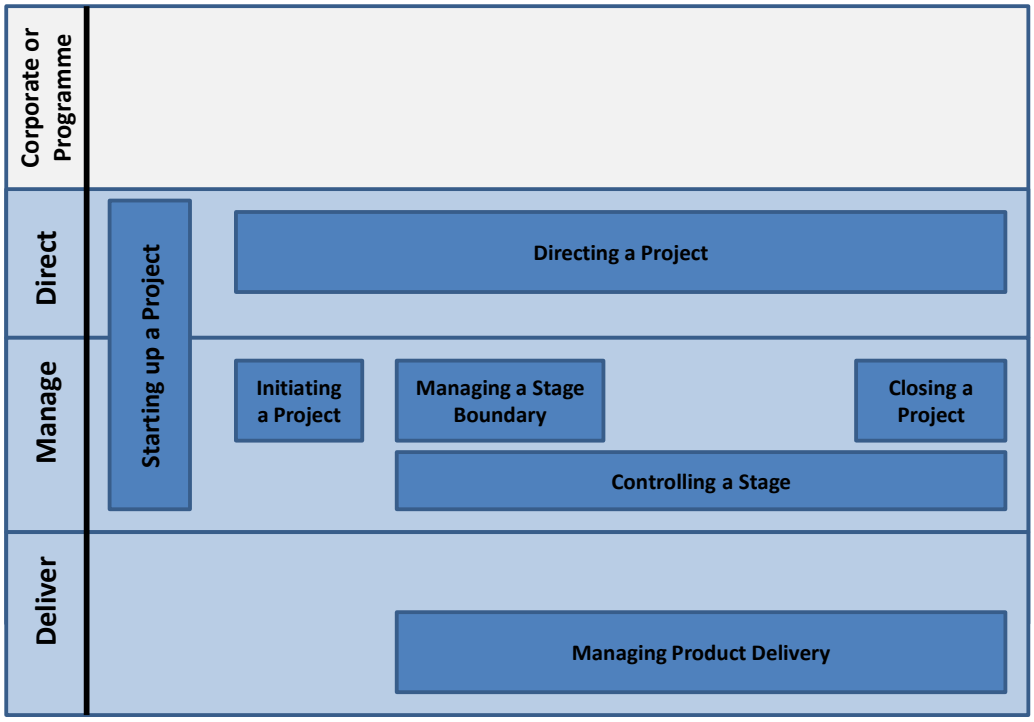


Figure 2.4: PRINCE2 processes in project management context

- Starting up a project. This process is aimed at ensuring that all the prerequisite elements for initiating the project are in place.

- Directing a project. This process is intended to enable the Project Board to direct and control the project through its life.
- Initiating a project. This project process establishes foundations for the project, including preparation of risk, configuration and quality management strategy, setting up project controls, project planning and refining the business case.
- Controlling a stage. For each defined stage of the project, this process is applied, including assigning work, responding to issues, reporting progress to higher management levels, and taking actions as necessary to ensure the stage proceeds within established tolerances. Work packages are authorised, their status reviewed and ultimately completed.
- Managing product delivery. As with controlling a stage, this process is repeated at each stage, and comprises accepting a work package, executing that work package, and delivering the complete work package. Team plans are created in this process, in parallel to the Stage plan.
- Managing a stage boundary. This process is completed at the end of a stage, where the project manager reports to the Project Board sufficient information to enable an assessment of the success of the stage and allow for continuation on to the next stage (as applicable) on the basis of a confirmation of continuing business justification. The business case is updated, and the next stage is planned and the Stage plan approved or exceptions identified.
- Closing a project. At the conclusion of the planned work (or alternatively, if the business justification no longer exists to continue the work), this process is executed. Activities that may be included are to prepare a planned (or premature) closure, hand over products, evaluate the project, and recommend project closure to the Project Board.

The fourth and final element of PRINCE2 is in tailoring the method to address environmental factors that impact the size, duration, organisational structure, type of project, sector or other aspects of the project. PRINCE2 accommodates various lifecycle models (e.g., waterfall, Agile), and the guidance for accomplishing these accommodations is included in the PRINCE2 method. Within this context, the PRINCE2 method discusses at length the concept of the evolving project, which is directly aligned with the Agile lifecycle model. In such scenarios, it may be implied that the tie-in between the specification for the development work and the business case is tenuous, as the specification evolves. Instead, the PRINCE2 approach suggests that the business case continues to evolve throughout the project life and thus keeps pace with the evolving specification.

APMG, accredited by the UK Accreditation Service as a certification body for PRINCE2 (amongst numerous other project management methodologies), accredits training organisations and training materials related to PRINCE2 Practitioner certification and provides PRINCE2 Professional certification.[40]

M_o_R®

PRINCE2 relies upon the OGC's Management of Risk: Guidance for Practitioners for an authoritative approach to managing risk. This approach is closely aligned with The Orange Book (refer to section 3.1.3 for a discussion of The Orange Book). The main risk management principles introduced in M_o_R® include:

[40] http://www.apmg-international.com

- Aligning the risk management work with the objectives of the organisation. This principle recognises that risk management ought to focus upon those elements of risk that have the potential to impact organisational objectives, whether strategic, operational, or at the programme level. This principle recognises the need to determine both the capacity the organisation has for risk as well as its risk appetite.
- Understanding and fitting within the current context. This principle is aimed at matching the risk management work to the current, both internal and external, context. The risk management approach is thus scaled according to the context.
- Involving stakeholders and introducing varying perceptions of risk. This risk management principle aims at engaging stakeholders proactively, improving the risk management work by getting their input to plans, understanding their perspectives regarding risks and their consequences. This principle recognises the need to engage with both internal and external stakeholders.
- Ensuring that risk management practices are clear and coherent so that stakeholders will benefit from guidance provided. This M_o_R principle aims to avoid a solution that relies upon standardised "tick-boxes" while still ensuring consistency in application of risk management practices.
- The outputs of risk management help to inform decision-making in the organisation. Thresholds, or risk tolerance, are determined and mechanisms are in place to create an escalation when exceeded. Various mechanisms may be brought to bear, including KPIs (key performance indicators) and EWIs (early warning indicators). Relying on such mechanisms ensure that risks are explicitly considered in the decision-making process.
- Risk management practices include ones that enable continual improvement. Making use of lessons learnt, including data that provides for cost-benefit assessments, help to ensure that similar mistakes are not repeated, or opportunities are not passed by.
- Creating a culture that supports risk-taking in alignment with the organisation's risk appetite. Excessive risk avoidance and excessive risk taking may be challenged equally within a supportive culture, which recognises the need for proactively managing risk.
- Establish measures of both process and performance that aim to achieve organisational value. Baselines and processes aimed at measuring performance are established, ensuring that investments in risk management work is justifiable.

In addition to these basic principles, the M_o_R® is implemented and adapted to an organisation. As a central part of this implementation, the M_o_R describes three main elements of documentation to be created, including a risk management policy, a risk management process guide, and strategies.

- The development of the risk management policy may be tailored to fit (though consistently) operating divisions within an organisation, portfolios of programmes, etc., and aims to establish a common language for risk management work.
- The risk management process guide identifies the steps to be followed to implement the risk management policy effectively.
- The risk management strategy is specific to a distinct organisational activity, describing the particular risk management activities that will be used.
- Other documents related to the implementation of the risk management strategy, are:
- the risk register, which is used to capture and maintain information on identified threats (and opportunities)

- the issue register, which maintains information on identified issues that require action,
- the risk improvement plan, which aims to assist in the process of embedding risk management within the organisation
- the risk communications plan, which identifies how information about risks will be interchanged with stakeholders
- the risk response plan, which is linked to the risk register, and outlines the specific details for responding to the occurrence of a particular risk event or group of events, and
- the risk progress report, which provides information on risk management to management personnel.

The M_o_R process consists mainly of four steps which occur in an ongoing cycle: identify, assess, plan, and implement. A separate activity, communicate, is identified outside of this cycle, reflecting the need to communicate with management or other stakeholders at any point within the process cycle. The M_o_R process also includes activities to embed and continually review the risk management work within the organisation, programme, or project, and all are guided by the M_o_R principles described above. These relationships are illustrated in Figure 2.5.

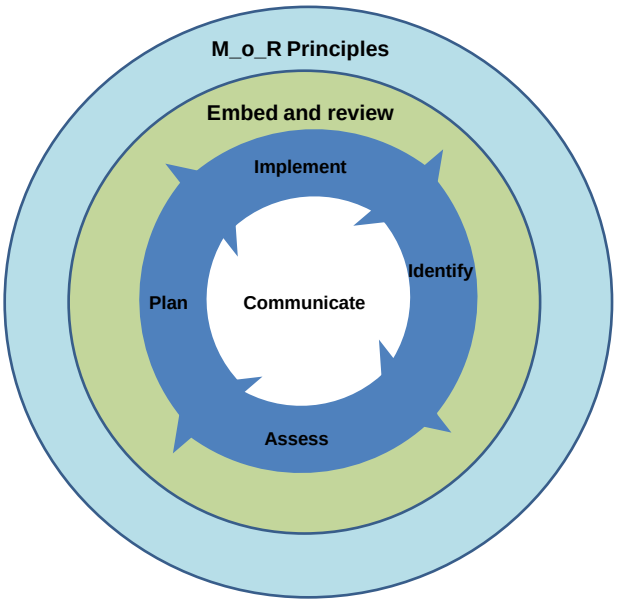


Figure 2.5: M_o_R process[41]

For each process step, goals are established, inputs and outputs identified, and tasks required to transform inputs to outputs described. Recognised risk management tools and techniques are also described for each process. The main processes described by M_o_R are:

- Identify-Context. Determine the objectives and scope for the activity, as well as identify any assumptions that have been made. Numerous techniques are identified for this process, which may include one or several of the following (or similar, alternative analytical approaches): stakeholder analysis, PESTLE (Political,

[41] Rendering based upon: Office of Government Commerce, *Management of Risk: Guidance for Practitioners*, p. 29, TSO, 2010.

Economic, Sociological, Technological, Legal, and Environmental) analysis, SWOT analysis, horizon scanning, probability impact grid.

- Identify-Identify the Risks. Identify specific risks to the activity with a focus upon the need to minimise threats and maximise opportunities. Within this process, a risk register is produced, and KPIs and EWIs prepared. Specific techniques suggested include checklists, cause and effect diagrams, group techniques such as brainstorming, Delphi, nominal group technique, constraints analysis, and others.
- Assess-Estimate. After risks have been identified, the probability of the occurrence of each threat or opportunity is estimated, as well as its potential impact and the time frame within which it would be likely to occur. Probability assessment, impact assessment, proximity assessment and expected value (or expected monetary value - EMV) assessment are techniques suggested for this process.
- Assess-Evaluate. The aggregation of identified threats and opportunities are assessed in this step, aiming to define the overall risk exposure. The process uses techniques such as risk profiles, probability trees, sensitivity analysis, and probabilistic risk models to arrive at this overall assessment.
- Plan. Preparation of specific responses to threats and opportunities (reduce threats/maximise opportunities). This process employs risk response planning, cost-benefit analysis, and decision trees to build a risk model.
- Implement. Ensure planned actions are implemented, include monitoring activities. The techniques used in this process are ones that update the summary risk profiles developed in the Assess-Evaluate process, as well as following risk exposure trends.

	Questions for project management methodology based on touch points	**Evidence from PRINCE2 method**
1	Does the PM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	PRINCE2 does not specify any provisions regarding compliance, rather, it focuses upon the products of the project, which are driven by the business justification. However, the risk management strategy of PRINCE2, based upon the separately published M_o_R Guidance, does provide for a framework within which risks such as those related to compliance may be addressed.
2	Is the PM methodology regarded as a process or is it simply about producing a report?	The PRINCE2 method includes a large number of specified documents, which are intended to be produced to frame, guide and control cyclical processes within a project. The M_o_R provides explicitly for a cyclical process to identify, assess, plan, and implement risk management activities. It also includes a number of specific documents in support of these activities, but the outputs are not limited to reports.
3	Does the PM methodology address only information privacy protection or does it address other types of privacy as well?	There is no treatment of privacy in this generic method (either within PRINCE2 or M_o_R).
4	Does the PM methodology say that it should be undertaken when it is still possible to influence the development of the project?	There is a significant focus on addressing issues related to risk in the early development of a risk management strategy, and in the continual checking and confirming of all

	Questions for project management methodology based on touch points	Evidence from PRINCE2 method
		aspects of the business justification, the product emerging from each stage, and the adjustment of future stages as each one approaches. Application of M_o_R process is cyclical and provide for continual improvement and reassessment.
5	Does the PM methodology place responsibility for its use at the senior executive level?	PRINCE2 is recommended to be embedded at the organisational level, and defines very specific roles and responsibilities for corporate or programme management, which may include senior executives. Business stakeholders are included as key contributors and expected to confirm the business justification for the project on a cyclical basis.
6	Does the PM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	PRINCE2 does call for developing different levels of plans: the overall project plan, and as each stage approaches, a more detailed Stage plan and Team plan. In addition, a specific plan to address risk is developed in the context of M_o_R, with the risk register as a critical output, identify risks, assessing and quantifying risks on and individual and aggregate basis, and defining strategies to minimise threats and optimise opportunities.
7	Does the PM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	A theme of PRINCE2 is in the area of lessons learned, where the project team is expected to study lessons from prior internal or external projects, or from other stages within the project.
8	Does the PM methodology include provisions for scaling its application according to the scope of the project?	One of the four main elements of the PRINCE2 method is for tailoring the method based upon environmental factors such as scope and size of the project. The M_o_R principles are tailored to scope to ensure proper application of risk management work, and appropriate use of resources.
9	Does the PM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	Both the principles of PRINCE2 and the themes that are linked to the processes within the method are aimed at recognising the three main stakeholders (business, user and supplier) or project interests. The Organization theme addresses working with and engaging stakeholders. One of the principles of M_o_R is for engaging stakeholders, both internal and external, to gain these types of insights, and to understand various perspectives of risk.

	Questions for project management methodology based on touch points	Evidence from PRINCE2 method
10	Does the PM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	A highly structured method for communication between management levels, based upon management by exception, is defined in PRINCE2. Acceptance criteria are defined at each stage of the project and the Project Board cyclically re-evaluates the business justification at each new stage to confirm the value of products emerging from the stage and the continued value of the project. M_o_R calls for a risk communication plan to explicitly define how information will be disseminated and inputs from stakeholders processed effectively.
11	Does the PM methodology call for identification of risks to individuals and to the organisation?	Yes, in part. That is, the M_o_R process is robust and provides a framework for identifying threats (as well as opportunities) to the organisation, the project and the product. However, as the approach is applied, risks related to individuals would need to be identified and emerge from the business case.
12	Does the PM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	PRINCE2 provides for identification of risk, but also of "dis-benefits" of the project, that is, the concept of known, expected negative impacts of the project, which may be objectionable to particular stakeholders, which would need to be considered in the business justification of the project.
13	Does the PM methodology include provisions for documenting the process?	Extensive documentation is included in the method, from a broad project plan to daily registers where issues and risks are identified and their resolutions addressed. In addition, the M_o_R calls for overall risk management policy, process guide, risk registers, issue registers, and various related documentation elements to enable improvement and monitoring.
14	Does the PM methodology include provision for making the resulting document public (whether redacted or otherwise)?	There is no specific provision for publication of the documents except between specific layers of the project management organisation.
15	Does the PM methodology call for a review if there are any changes in the project?	The PRINCE2 method calls for continual revision and updates to the business justification for the project as it moves from one stage to the next.
16	Does the PM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	There is no specific provision for audits, but at the completion of each stage of the project, verification activities are prescribed in the Managing a Stage Boundary process where audit requirements could be introduced. The M_o_R process calls for a cyclical re-evaluation and assessment of risk.

Conclusions and recommendations

The PIA process, integrated into a specific business environment where the PRINCE2 method is applied, could be addressed within three specific contexts:
1. In the Business Case theme, privacy standards could be established as overarching requirements that must be achieved in all products and thus built into the business justification.
2. In the Organization theme, stakeholders representing the privacy rights of individuals could

Manifesto for Agile Software Development

We are uncovering better ways of developing software by doing it and helping others do it.
Through this work we have come to value:

Individuals and interactions over processes and tools
Working software over comprehensive documentation
Customer collaboration over contract negotiation
Responding to change over following a plan
That is, while there is value in the items on the right, we value the items on the left more.

Twelve Principles of Agile Software Development

1. Our highest priority is to satisfy the customer through early and continuous delivery of valuable software.
2. Welcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage.
3. Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.
4. Business people and developers must work together daily throughout the project.
5. Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done.
6. The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.
7. Working software is the primary measure of progress.
8. Agile processes promote sustainable development. The sponsors, developers, and users should be able to maintain a constant pace indefinitely.
9. Continuous attention to technical excellence and good design enhances agility.
10. Simplicity--the art of maximizing the amount of work not done--is essential.
11. The best architectures, requirements, and designs emerge from self-organizing teams.
12. At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly.

be included in the engagement activities.
3. In the Risk theme, privacy and data protection could be included as risks to be evaluated, and PIAs introduced as a technique for evaluating and controlling these risks. The specific techniques should be introduced in the M_o_R which is a companion to the PRINCE2 method.

2.2 TECHNOLOGY DEVELOPMENT MANAGEMENT METHODOLOGIES

2.2.1 Agile

The Agile software engineering movement traces its origins to a 1986 article that proposed the game of rugby as a model for team effectiveness, with the team members passing the ball

back and forth as they move down the field.[42] As Agile methods began to develop in software engineering through the 1990s, more formal methodologies based upon these ideas started to emerge. The Agile Manifesto and its explicating principles were written by a group of 17 developers in February 2001[43], and have served as a launch pad for the formalisation of numerous Agile methodologies.

While there are numerous specific methodologies based upon Agile, in general, they all focus upon the following common elements:

- teams – encouraging effective working teams
- meeting user needs – the user is a key member of the team
- developing shippable product – that is, even if the software is not delivered to the end-user, whatever *is* developed is "done" and ready to be delivered
- fast and frequent cycles – development is completed in short sprints or iterations that are typically time-boxed from 1 – 4 weeks in length.

In a growing number of large and small organisations, and particularly those operating within the digital economy, Agile development methodologies are replacing a traditional waterfall development approach. Recent market surveys have shown a trend towards broad adoption of Agile methods (34% of those surveyed in a 2012 PWC survey[44]; 35% in a 2010 Forrester Research survey[45]). In a survey of developers at Nokia[46], where there has been an organisation-wide transformation to agile methods, for those individuals who had been using the methods, 60% indicated that they would not choose to "go back to the old way of working", suggesting that there is a strong commitment at the grass roots level.

While gaining in popularity, and entering the mainstream, Agile methodologies are often used in hybrid implementations alongside more traditional project management methodologies in large enterprise settings. Where Agile itself offers a more philosophical view of development, methodologies such as Scrum[47], Crystal[48] and XP (eXtreme Programming)[49] are generally followed as guides to development processes. Other methodologies that provide for the application of agile approaches include Feature Driven Development (FDD)[50], Test Driven Development (TDD)[51], Adaptive Software Development (ASD)[52], Agile Modeling (AM)[53], Dynamic Systems Development Method (DSDM)[54], and Lean Development[55].

---

[42] Takeuchi, Hirotaka, and Ikujiro Nonaka, "The New Product Development Game", *Harvard Business Review*, Vol. 64, No. 1, January 1986, pp. 137–146. http://hbr.org/1986/01/the-new-new-product-development-game/

[43] Kent Beck, Mike Beedle, Arie van Bennekum, Alistair Cockburn, Ward Cunningham, Martin Fowler, James Grenning, Jim Highsmith, Andrew Hunt, Ron Jeffries, Jon Kern, Brian Marick, Robert C. Martin, Steve Mellor, Ken Schwaber, Jeff Sutherland, Dave Thomas, February 2001. www.agilemanifesto.org

[44] PriceWaterhouseCoopers, *Insights and Trends: Current Portfolio, Programme, and Project Management Practice*, The third global survey on the current state of project management, 2012.

[45] West, D., and T. Grant, *Agile Development: Mainstream Adoption Has Changed Agility*, Forrester Research, 20 January 2010.

[46] Laanti, M., Salo, O., and Abrahamsson, P., "Agile methods rapidly replacing traditional methods at Nokia: A survey of opinions on agile transformation", Information and Software Technology, 53: 276-290, 2011.

[47] Schwaber, K., and M. Beedle, *Agile Software Development with SCRUM*, Prentice-Hall, 2002.

[48] A. Cockburn, *Crystal Clear: A Human-Powered Methodology for Small Teams*, Addison Wesley, 2004.

[49] Beck, K., *Extreme Programming Explained: Embrace Change*, Addison-Wesley, 1999.

[50] Palmer, S.R., and J.M. Felsing, *A Practical Guide to Feature-Driven Development*, Prentice Hall, 2002.

[51] Beck, K., *Test Driven Development: By Example,* Addison-Wesley Longman, 2002.

[52] Highsmith, J.A., *Adaptive Software Development: A Collaborative Approach to Managing Complex Systems*, Dorset House, New York, 2000.

[53] Ambler, S., *Agile Modeling: Effective Practices for eXtreme Programming and the Unified Process,* 2002.

[54] Craddock, et al, *The DSDM Agile Project Framework for Scrum*, DSDM Consortium, 2012.

These methodologies have each emerged from Agile principles, translating the general principles into practical application. Scrum is the methodological interpretation of Agile that enjoys the widest adoption of these and some of the key concepts of this lightweight methodology (many of which have parallels in the other methodologies) include the following:

Scrum – key concepts[56]	
Product backlog	The product backlog is a list of product features that need to be developed. These features are typically described as **user stories** that define what the user needs and why it is important. **User stories** are assigned points that reflect their complexity. The story points are assigned during a process called backlog grooming. A large user story is referred to as an **Epic**. Once all the user stories and their points are accumulated, the product backlog is "burned down" over the ensuing development periods (sprints), where the work is completed on a basis of priority, as defined by the user.
Sprint planning & backlog grooming	**Backlog grooming** is a process undertaken by the team to evaluate each user story, assign points, and if the number of points are considered to be too large, to break a user story down into multiple user stories that are of a more manageable size. As the backlog is groomed, the user also sets the priority for stories in the backlog, and the work to be done by the team is selected from these prioritised stories as a **sprint planning** exercise. The work selected will be done over a specific, consistently time-boxed period (from 1-4 weeks), which is called a sprint, and generally, the total number of user story points included in a sprint is consistent from one sprint to the next.
Sprints or iterations	A sprint or iteration is a time-boxed period focused upon completing the prioritised product backlog items, with the team (usually co-located) working toward achieving daily goals, and applying Agile development techniques. During the course of the time-boxed sprint, reviews of progress are performed in the daily scrum.
Scrum or daily stand-up	**Scrum** is a daily event for each team. Team members are called upon to answer three questions[57]: • What did I accomplish since the last daily scrum? • What do I plan to work on by the next daily scrum? • What are the obstacles or impediments that are preventing me from making progress? Anyone who is not a part of the team is not expected to contribute to the scrum. Often the scrum is a stand-up meeting to promote brevity, is always time-boxed (usually 15 minutes) and one individual, the **ScrumMaster**, acts to ensure the rules of the scrum are respected.

[55] Poppendieck, M., and T. Poppendieck, *Lean Software Development: An Agile Toolkit*, 2003.
[56] Rubin, K.S., *Essential Scrum : a practical guide to the most popular agile process*, July 2012; Schwaber, K., and M. Beedle, op cit.
[57] Cobb, C.G., *Making sense of agile project management : balancing control and agility*, John Wiley & Sons, Inc., Hoboken, NJ, 2011.

Scrum – key concepts[56]	
	The team members are typically co-located in an open room to encourage frequent and constant interaction, often including pair programming. If any issues are raised in the daily scrum that require follow-up, this is done after the meeting in this collaborative setting.
Sprint review	Towards the end of a sprint, there is a sprint review meeting in which the team meets with the product owner to review the potentially shippable product, inspecting and adapting it based upon the review discussions. The sprint review will be followed by a **sprint retrospective** where the team will meet to discuss process and adapt for future sprints.
Burn-down	During the course of each successive sprint, tracking of progress is done by following the points associated with user stories that have been completed. Thus, if the product backlog began with 4000 points from the collected and prioritised user stories, each sprint may "burn down" 200 or 300 of those points (in a large project, multiple teams will work on different user stories in the backlog with each contributing to the burn-down). With each successive sprint, the outstanding points in the backlog is reduced and charted. The focus is upon reducing the product backlog (though new stories may be added along the way, increasing the total size of the backlog), and typically, the team will have a board displaying the burn-down in their work area.

Doneness	Doneness is a key concept in that, for each sprint, a team evaluates whether the developed software achieves the user needs expressed in the user stories, as well as whether it meets other, broader goals.
	
	Doneness criteria is established during the initial sprint of a project, and will typically include several layers and types. For example doneness definitions typically include organisational, product, and team layers and doneness criteria that are applied at different stages of development (e.g., story, feature, product version). Examples (not a comprehensive list) of different types of doneness criteria at successively more specific layers include:
	• Organisational layer
	  ○ coding standards
	  ○ compliance with overarching industry regulations
	  ○ types of required testing and required status
	  ○ compliance with UI standards
	  ○ procedures to store completed documentation and records
	  ○ requirements for copyright, service marks, logos, etc.
	• Product layer
	  ○ standards or regulations specific to the product (e.g., those related to medical devices)
	  ○ completion of automated testing using an approved testing tool
	  ○ specific performance requirements
	• Team layer

Scrum – key concepts[56]	
	○ independent validation of completed stories by team members ○ peer review requirements for code are met In addition to these layers, each story will have extensive doneness criteria that determines what must be done (testing, updating, refactoring, etc.) to consider a specific story completed or an identified defect resolved. If, at the end of a sprint, a user story is determined to be not done, it goes back into the product backlog and will be considered where to include it in subsequent sprints. In addition, feature doneness will determine the criteria for a product feature (which may include several stories), and version doneness is applied when a product version is completed (collection of features). In each case, the criteria will be applied across the organisation, product, and team layers. The most appropriate level for consideration of how privacy and data protection fits into the concept of doneness is within the organisational layer, alongside regulatory requirements that are applied to the organisation as a whole. Due to the need to develop a definition of doneness in the initial sprint for a project, there exists an opportunity to develop knowledge around privacy and data protection requirements and to develop a privacy aware culture. The review of doneness criteria at the close of each sprint provides a reinforcing impact of the privacy-related criteria.

The inter-relationships of these Agile elements are illustrated in Figure 2.6.

Other Agile methodologies include many of these same elements, though sometimes referred to by different names. For example, XP focuses more on the specific approaches to development of code, including the development of user acceptance tests as related to the writing of user stories (i.e., almost concurrently), pair programming, refactoring and test-driven development (writing the test before the code).

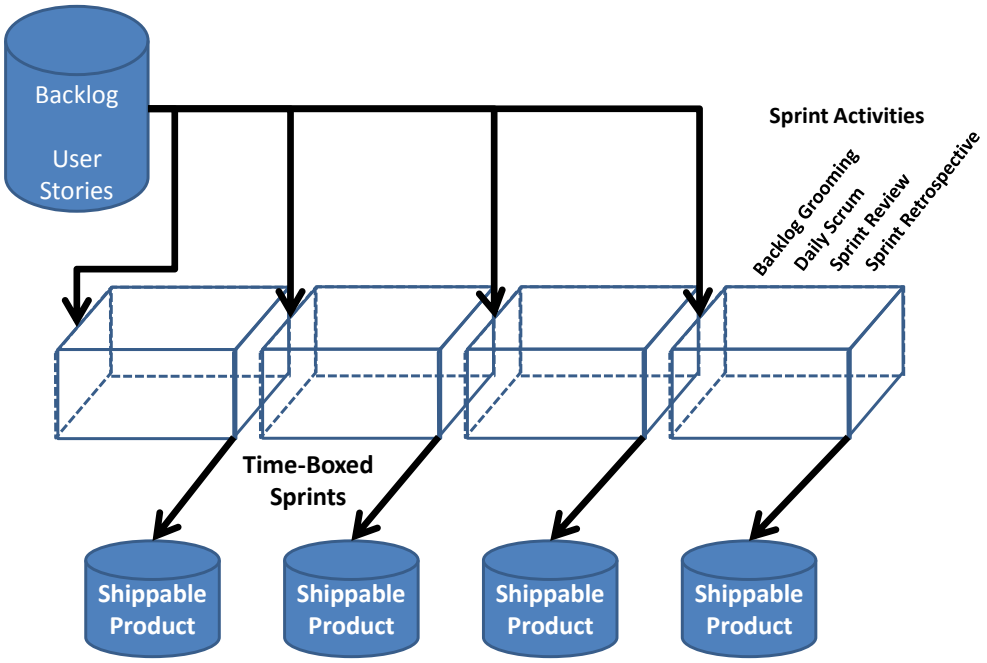


Figure 2.6: Relationships amongst Scrum methodology components

Real world application of Agile methodologies

A great deal of literature can be found to describe how Agile methodologies are applied in practice, and how they can be effectively introduced into an organisation from small development teams[58] to large enterprises[59]. Part of the complexity in implementing Agile methodologies is that the methodology itself diverges significantly from more traditional SDLC (software development life cycle) approaches, and the shift away from those approaches requires an equally significant culture shift. Rather than focusing upon specific tasks in a WBS that need to be completed in a particular sequence, the focus is entirely upon the product that needs to be created and how the user would like the product to look, function, operate. It is expected that the user will shift their priorities and rethink their own requirements over the course of the development project, and thus, the specific details of what the product will be, when it will be complete, and what it will look like will evolve with the user's requirements.

Using the Scrum methodology concepts described above, the following sequence would typify an Agile project:

1. The organisation defines a project to be undertaken. This is outside the Agile methodology, and any preliminary steps required to authorise resources for a project (e.g., making the business case) are not a part of the Agile development process. For example, it may be that the organisation uses PRINCE2 PM methodology, tailoring that methodology to encompass Agile processes within the framework.
2. The user defines the requirements in the form of **user stories** (or **epics**) to create the **product backlog**.

[58] Taylor, Philip S., Greer, D., Coleman, G., McDaid, K, and Keenan, F., "Preparing Small Software Companies for Tailored Agile Method Adoption: Minimally Intrusive Risk Assessment", *Software Process Improvement and Practice*, 13: 421–437, 2008.
[59] Schiel, J., *Enterprise-Scale Agile Software Development*, CRC Press, 2010.

3. At the beginning of the project, the user assigns **priorities** to the user stories, and along with the development team, scopes the work. In this process, **story points** are assigned that provide a sense of how much work is involved. Often, teams use special playing cards[60] to play "planning poker", for estimating and arriving at consensus on the scope of a particular user story (the special card decks typically have cards for ?, 0, 1/2, 1, 2, 3, 5, 8, 13, 20, 40, 100, infinity - and sometimes a coffee cup, used when it is time for a break).
4. The work is done in a series of time-boxed sprints (usually 1 to 4 weeks, but typically a consistent length of time over the course of the project). In the first sprint, more time is spent in planning efforts than in subsequent sprints, but in each one, this **backlog grooming** continues. The ongoing planning sessions are used to discuss the stories and refine estimates (stories that are too large are broken down into smaller pieces so they can be effectively estimated).
5. Within each sprint, the co-located team works together to develop the product, and on a daily basis, the team has a 15 minute meeting to report on what they have done in the past day, what they plan to do in the next day, and whether there are impediments that prevent them from making progress.
6. At the end of the sprint, a **sprint review** is conducted. The product is validated against the requirements. The development team indicates whether the product meets **doneness** criteria and after inspection in the sprint review, product may be accepted as done, or if rejected, placed back into the product backlog and reprioritised to be addressed in a subsequent sprint.
7. As the product backlog is depleted with the completion of shippable product in each sprint, the backlog is **burned-down**, and ultimately, project brought to conclusion.

A typical team room for an Agile team might have user stories on post-it notes on a wall, a whiteboard with task assignments and technical details, and a simple indicator of whether the current product build is working. A war room may be established for agile teams to use during backlog grooming, daily stand-ups, sprint reviews, and other meetings. Planning and estimation might be done with simple playing cards or tee shirt sizes. The emphasis in Agile is upon person-to-person communication and not on process related reports. That said, some reporting tools and other aids have evolved over time and continue to emerge, including a software-based version of planning poker[61], and adaptations of team software[62] to suit the Agile team.

It is also important to recognise that in those organisations where Agile methodologies are employed, specific elements are often selected to be implemented, while others are not applied. Forrester's most recent survey on Agile adoption indicates not only are individual components selected and others ignored, there is often a mix of Agile and non-Agile methodologies at the organisational level, deliberately mixing (39%) different Agile methodologies and deliberately mixing (35%) Agile and non-Agile methodologies.[63]

In order to effectively contemplate how PIAs, or for that matter, privacy and data protection generally, may be integrated into an Agile methodology, we look at three key elements:

---

[60] Technique popularised by publication of: Cohn, M., *Agile Estimating and Planning*, Prentice-Hall, November 2005.

[61] http://www.planningpoker.com/

[62] An example of using team software in an agile environment is found in a case study of Microsoft's Team Foundation Server: http://msdn.microsoft.com/en-us/magazine/dn189203.aspx

[63] West, D., and T. Grant, op. cit.

1. how risk issues are currently addressed by the methodology,
2. how to influence the methodology to ensure it addresses privacy and data protection,
3. how key PIA touch points are currently addressed in the methodology.

In Agile-based methodologies, contemplation of risk is focused upon impacts of not achieving the work defined for the sprint, not on broader organisational definitions of risk (such as those related to security, privacy or similar risks). The methodologies focus upon the effective, agile functioning of teams to develop products that have high levels of quality, and include shippable product as early as possible. Risk issues need to be addressed at a higher level, above that of the Agile team.

Although there is no standards board or body that acts in an authoritative role to define Agile methodology standards, there are a wide range of commercially accessible books and training courses to provide guidance to developers who wish to learn and hone their skills in applying Agile in practice (many referenced within this section). However, there has been an evolution on the certification front, with the development of some standards for training courses offered by many firms involved in project management training. The International Consortium for Agile, founded by one of the original authors of the Agile Manifesto, "builds learning roadmaps, accredits courses and trainers, makes those lists available to students, and offers certification and recognition to students as they progress. ICAgile does not evaluate, rate or prioritize the courses against each other, nor does ICAgile offer courses itself."[64] To impact these methodologies that have emerged on a grass-roots basis, trying to influence the International Consortium may be useful; however, many developers are practitioners of Agile methodologies without the benefit of such certifications.

Numerous case studies are available to provide clues not only as to how Agile is being implemented in real-world settings, but also to provide some ideas as to how issues of privacy and data protection might become integrated into an agile methodology.

In 2002, a development team of 120 in a Fortune 50 financial services company aimed to stabilise a large project that was significantly behind schedule by implementing XP (Extreme Programming) within an agile project management approach. As a part of the transition, the entire development team was trained in XP, with other breakout sessions tailored to subgroups.[65] *This experience suggests that when large organisations transition to Agile on a broad basis, it can provide an opportunity to introduce key concepts of doneness, including those related to privacy and data protection during team training* .

A 2012 case study[66] for a small software development company illustrates an evolution from traditional SDLC approaches to an Agile approach (Scrum). The published study illustrates the lessons learnt and overall metrics showing quality and cycle time improvements, as well as improved customer satisfaction levels. As a key part of their transition, the software firm engaged an Agile consultant to guide them in their process. *This illustrates the importance of ensuring that professional practitioners are educated in broad regulatory issues such as*

[64] www.icagile.com.
[65] Augustine, S., Payne, B., Sencindiver, F., and Woodcock, S., "Agile Project Management: Steering from the Edges", *Communications of the ACM*, Vol. 48, No. 12., December 2005.
[66] O'Connell, Etal, "Agile Case Study - Cayen Systems", 5 June 2012.
http://www.codeproject.com/Articles/394071/agile-case-study-cayen-systems

privacy and data protection as they have the opportunity to influence development teams in their approach.

There is some controversy within Agile circles about how to effectively launch a project. While many practitioners eschew any significant upfront planning, while others propose an inception phase, aimed at doing a level of planning and definition of scope prior to the first sprint. The inception phase is seen as an opportunity to integrate agile within the enterprise, particularly where other, more structured processes already exist. Authors Ambler and Lines of IBM[67] describe the Disciplined Agile Delivery (DAD) process framework as an effective approach to integrate agile in such environments, including aligning with the enterprise direction, development of the initial release plan, defining a common vision along with stakeholders, and identifying risks. *Within large enterprises, the inception phase can provide an opportunity to engage with a broad range of stakeholders and to ensure that issues related to privacy and data protection have been integrated into the shared vision.*

	Touch points questions	**Evidence from Agile methodology**
1	Does the PM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	There are no provisions for compliance with legislation or regulations in Agile methodologies, beyond the concept of doneness at the organisational layer.
2	Is the PM methodology regarded as a process or is it simply about producing a report?	Agile methodologies are collections of lightweight processes, but do not include any processes related to privacy.
3	Does the PM methodology address only information privacy protection or does it address other types of privacy as well?	There are no provisions in Agile methodologies with respect to privacy.
4	Does the PM methodology say that it should be undertaken when it is still possible to influence the development of the project?	Agile methodologies are open to change and adaptation through every stage of the product development. There is no explicit timing defined for any subsidiary process, audit or other work. All is to be defined and prioritised by the user.
5	Does the PM methodology place responsibility for its use at the senior executive level?	No. Agile methodologies are focused upon the development team and does not include the concept of management intervention or interaction with the team's work or priorities.
6	Does the PM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	Agile methodologies do continuous planning, identifying product backlog items to be completed in each iteration or sprint, grooming the backlog, and inspecting completed work and adapting the priorities. The only consultations included in these methodologies are with the user.

[67] Ambler, S., and Lines, M., *Disciplined Agile Delivery: A Practitioners Guide to Agile Software Delivery in the Enterprise*, IBM Press, 2012.

	Touch points questions	Evidence from Agile methodology
7	Does the PM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	No. There is no concept of an environmental scan in Agile methodologies.
8	Does the PM methodology include provisions for scaling its application according to the scope of the project?	No. The scope of work done in individual sprints is specifically limited to that which can be done by a development team over the time-boxed 1-4 week period. Larger scope elements are not considered and will be addressed on an ongoing basis as the product backlog is burned down.
9	Does the PM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	No. The user represents the perspectives of any stakeholders, though the methodologies do not distinguish between them (i.e., the user brings the overall perspective to the development team).
10	Does the PM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	The Agile methodologies call for typically co-located teams where a central board with information about product backlog, burn-down of user stories, or other goal focused communications are displayed. Senior management and other stakeholders are explicitly excluded from the communications process, and external views are brought by the user.
11	Does the PM methodology call for identification of risks to individuals and to the organisation?	No. Agile methodologies do not have a risk identification process. The only real examination of risk is within the context of ensuring that product backlog, in the form of user stories, is properly valued and estimated so that the risk of not completing the work within the duration of the sprint/iteration is reduced.
12	Does the PM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	No. These elements are not considered by the methodologies directly. These issues may be contemplated within the design and established as user stories or as criteria for doneness.
13	Does the PM methodology include provisions for documenting the process?	No. Agile methodologies eschew documentation, and only anticipate creating the minimum amount of documentation to enable the following sprint/iteration to be completed.

	Touch points questions	Evidence from Agile methodology
14	Does the PM methodology include provision for making the resulting document public (whether redacted or otherwise)?	No.
15	Does the PM methodology call for a review if there are any changes in the project?	Agile methodologies are intended to allow for continuous inspection and adaptation and is well suited to re-evaluate user stories or doneness criteria throughout the project.
16	Does the PM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	No. However, each sprint/iteration includes an opportunity to inspect product and adapt. A user story (or stories) may be written and inserted into the product backlog to implement the PIA recommendations.

Conclusions and recommendations

Within the Agile methodologies, there is no specific concept for embedding privacy and data protection principles in software development work to be completed; thus, we recommend that two potential approaches be considered for embedding or inserting these successfully in Agile methodology based projects:

Option A: Approach PIAs as a specific element of the product backlog.

A user story or stories could be written to identify how privacy and data protection principles should be included within the context of the product and inserted into the product backlog. This may prove challenging to implement, depending upon the specific product being developed and its complexity. For example, the user story may be written to require the completion of a PIA of the software. The problem with this approach is that shippable pieces of software are constantly being developed over the course of multiple sprints. If a PIA is performed early in the project, and significant changes are made later in the project, the results may be invalidated or undone. If a PIA is performed late in the project, there is the potential for the need to significantly alter the product, creating risk to meeting time, cost and quality-based goals.

Option B: Approach PIAs as an organisational standard for "doneness".

On an organisational level, privacy and data protection requirements would be defined as a standard, and these requirements should be included in the definition of doneness at the organisational layer for all software development activities. This approach would require a significant effort to establish the requirements in a way that can be effectively applied to a broad range of development activities, and should involve efforts to train all Agile developers to understand how these principles are to be applied and thus evaluated within the definition of doneness. User acceptance tests would need to be designed to reflect the defined privacy and data protection standards. PIAs would not be performed within the context of the project, but theoretically could be performed at any time during the course of the project to ensure that privacy and data protection requirements are consistently achieved. Where they are not, the organisational standards may need to be revisited and modified to ensure greater alignment,

and user stories written to correct any problems discovered. The PIA would thus be transformed from a periodic event to a continuous validation of privacy standards.

Given the grassroots origin and developer-driven adoption of Agile, finding opportunities to introduce and encourage a privacy culture within the Agile context may present particular challenges not found with highly structured methodologies emanating from a central standards body or certification board. Reaching developers will require efforts on several fronts, including the training bodies mentioned above, but also via the same grassroots communities that have helped to advance the key concepts of XP, Scrum, and others. Message boards and discussion groups, Agile consultancies that specialise in helping organisations integrate Agile in their environment, training organisations that provide public and organisation specific training courses -- all of these should be targeted as hubs for the communication of privacy and data protection needs that need to be met to protect individuals and the organisation.

2.2.2 HERMES

HERMES[68] stands for "**H**andbuch der **E**lektronischen **R**echenzentren des Bundes, **M**ethode für die **E**ntwicklung von **S**ystemen". It is an open standard and method for the "management and execution of projects" in the area of Information and Communication Technologies (ICT). It was developed by the Swiss Federal Strategy Unit for Information Technology (FSUIT) for use in the Swiss federal administration. It has its roots in the early 1970s with a first official release in 1975. Then, it was extensively revised in years 1986 and 1995 and the current version of the method dates from 2003 with an expected new version "HERMES 5" in 2013.

Today, HERMES is also used outside the Swiss federal administration, at the regional level and by schools and private companies, as well as by international organisations and foreign public administrations such as that of Luxembourg.

HERMES' main reference documents are available in German and French. They consist of the "HERMES Foundation", 38 pages long, (which is also available in English[69]) and two manuals for two specific cases. The first one "HERMES Manual, Project type: System Development" concerns the development of new software applications and the second one "HERMES Manual, Project type: System Adaptation" concerns the purchase and the adaptation of new software applications.[70] Also available is "HERMES Manager – Pocket guide"[71] which describes the project management method and its application from the manager's point of view. Finally, HERMES' user group, hosted by eCH,[72] has also produced a set of documents about HERMES and ITIL, HERMES and Agile, and a HERMES manual for organisation management.[73]

---

[68] http://www.hermes.admin.ch

[69] Hermes, Management and Execution of projects in Information and Communication Technologies (ICT), Foundations, 2003. http://www.hermes.admin.ch/ict_project_management/manuals-utilities/manuals-for-downloading/hermes-foundations/at_download/file

[70] Both manuals are only available in German and French. http://www.hermes.admin.ch/ict_project_management/manuals-utilities/manuals-for-downloading

[71] In English. http://www.hermes.admin.ch/ict_project_management/manuals-utilities/manuals-for-downloading/hermes-manager-pocket-guide/at_download/file

[72] eCH is the Swiss Association for E-government Standards. http://www.ech.ch

[73] Those documents are only available in German and French.

HERMES applies to all of the participants in a project, whether the purchaser or the supplier. As a method for management and execution of projects, it mainly targets the project leaders as well as the management staff. However, it also provides guidance for the other project participants to support their successful involvement.

HERMES is goal- and results-oriented. Its main approach is to structure the development and the execution of a project by clearly and deeply providing specifications for the project's expected results, from which all activities and responsibilities are then derived. This clear results-orientation should avoid unnecessary activities and contribute to better efficiency. In this regard, HERMES' noticeable characteristic is to use a three-dimensional approach:

1. view to obtain results (What)
2. view to procedures (How)
3. view to the various roles (Who).

In this approach, results, procedures and roles are fully interdependent and linked together. Any objective within a project must combine all three to be achieved. Activities and work steps are combined together in the so-called "Work Breakdown Structure" (WBS) which is a step-by-step description of what needs to be done, how and by whom.

In the project management area, HERMES belongs to the traditional "waterfall" model which is a sequential design process where the "progress is seen as flowing steadily downwards (like a waterfall) through the phases of Conception, Initiation, Analysis, Design, Construction, Testing, Production/Implementation, and Maintenance".[74] HERMES is clearly a phase-oriented project management and execution method. HERMES has six main phases; however, their contents and names may differ according to the type and/or size of the project. For instance, in the case of "System Development", the six phases are: Initialisation, Pre-analysis, Concept, Implementation, Deployment and Finalisation. For each phase, "Decision-Making Points" are set out. They materialise HERMES' results to be obtained and they form the basis on which decisions are taken to go from one phase to the next.

HERMES also provides a description for overlapping and concomitant tasks required for guaranteeing a project's success. Those specific tasks are summed up in sub-models which span the project's development cycle. The five main sub-models are: Project Management, Risk Management, Quality Assurance, Configuration Management and Project Marketing, as shown in Figure 2.7.

http://www.hermes.admin.ch/services/utilitaires-1/Etudes%20-%20Brochures

[74] https://en.wikipedia.org/wiki/Waterfall_model

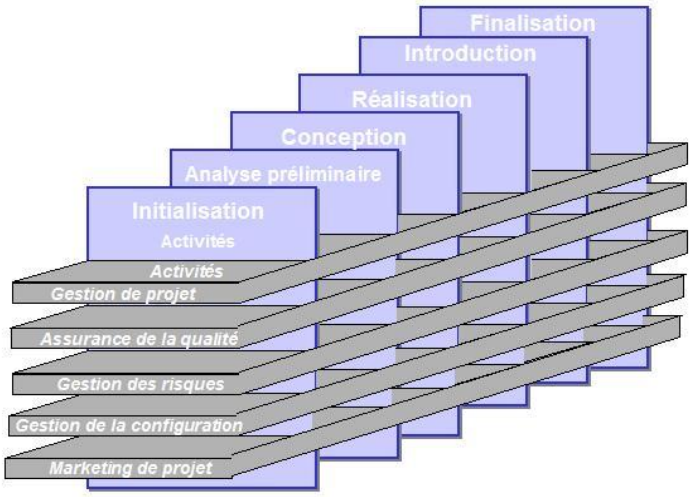


Figure 2.7: HERMES' phases and sub-models organisation[75]

HERMES is notably suited for system development as well as system adaptation for which two manuals exist. However, it also includes provisions for project-specific procedures within its "Tailoring" feature.

Two levels of certification schemes are available. The first one, HERMES Swiss Project Team Professional (HSPTP), addresses the needs of all project participants. The second one, HERMES Swiss Project Manager (HSPM), targets the project head. Until now, both certification schemes are carried out by the Swiss Association for Quality (SAQ).

With regard to the question about how to integrate PIA methodology within this project management methodology, HERMES has advantages. The first one is its task on Information Security and Data Protection (ISDP) which is in two parts:

- Information security, with respect to confidentiality, integrity and availability, of the data handled by the software or the system being developed;
- Specific attention for personal data and all requirements set forth by the Swiss Federal Data Protection law enacted in 1992.[76]

The second one is HERMES' Tailoring feature which opens a door for adding specific new objectives and their corresponding work steps leading to the expected results regarding privacy protection as set out in PIAs. The third one is constituted by the sub-models on Quality Assurance (QA) and Project Marketing (PM). The former includes provisions for guaranteeing that all of the necessary audits and tests are planned, prepared, effectively and comprehensibly carried out and adequately documented. The latter includes the necessary provisions for communication inside and outside the project with the following main targets: the purchaser, users, operators and project team. However, there is little or no evidence about

75
http://www.gestiondeprojet.lu/cms/gestiondeprojet/publishingfr.nsf/646184f03288e928c1257035004f3542/8aa1a3c518dd0ddcc12578220043073d!OpenDocument&ExpandSection=3,1#_Section3

76 http://www.admin.ch/ch/e/rs/c235_1.html

other types of stakeholders' involvement, although this limit could easily be overcome by including the missing ones during the Tailoring step.

Finally, within HERMES, the risk management sub-model mainly deals with all of the risks regarding project achievement but not the risks induced by the project itself on the users. Like the above, this could easily be overcome during the Tailoring step.

	Touch points questions	Evidence from HERMES
1	Does the PM methodology include provisions about compliance with legislation and any relevant industry standards, codes of conduct, internal policy, etc.?	HERMES includes provisions for a general compliance within the Quality Assurance (QA) sub-model. This sub-model starts with the Initialisation phase, that is, at the beginning of the project. The QA describes all the necessary requirements to achieve the level of quality for the success of the project as well as the required verifications and audits to ensure the demands are met. HERMES also lists some key factors which can contribute to the success of the project, some of which include provisions for compliance. These are: 1. "Project Environment", which takes into account the organisation's environment in which the project takes place, i.e., its policies, standards, etc. 2. "Information security and data protection", which makes specific provisions for compliance with the Swiss Personal Data Protection Act. 3. "Ecology", which makes specific provisions for taking into consideration all environmental legislative requirements which could impact the project.
2	Is the PM methodology regarded as a process or is it simply about producing a report?	HERMES is a process-oriented, project management method. HERMES is all about the development of a project, from the expression of needs to its deployment and finalisation. HERMES results in the production of a lot of documentation at all stages of the project development cycle.
3	Does the PM methodology address only information privacy protection or does it address other types of privacy as well?	HERMES has no provision for different types of privacy protection other than personal data protection. Personal data protection is handled within a specific task, i.e., the information security and data protection (ISDP) task. This task makes provision for considering the requirements set out by the Swiss Personal Data Protection Act.
4	Does the PM methodology say that it should be undertaken when it is still	HERMES is all about the development of a project. Hence, it must be started at the

	Touch points questions	Evidence from HERMES
	possible to influence the development of the project?	beginning of the project.
5	Does the PM methodology place responsibility for its use at the senior executive level?	HERMES calls for the organisation's senior management to support fully the project manager.
6	Does the PM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	As a starting point for the project, HERMES requires a project mandate which should include the first draft of the project's terms of reference and the project plan. Those documents will continually evolve during the project and will include provisions for some consultation with the project participants.
7	Does the PM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	HERMES requires a project environment analysis. This is among its key factors which can contribute to the success of a project. However, this analysis mainly concerns the organisation's context in which the project will take place rather than similar projects from which lessons could be learned. During the pre-analysis phase, HERMES makes provision for a wide analysis of the project's issues and their possible solutions.
8	Does the PM methodology include provisions for scaling its application according to the scope of the project?	HERMES includes provisions for adapting itself to the scope and size of the project, thanks to its Tailoring feature. This feature provides the necessary tools and rules to focus only on the necessary tasks to achieve the expected results.
9	Does the PM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	HERMES only refers to consulting relevant stakeholders from the project development perspective to draw the project's specifications and its requirements. There is little or no evidence of assessing the project's impacts.
10	Does the PM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	Among the key factors which can contribute to the success of a project, HERMES includes communication with all project participants. Inside the project, this communication must scale with the project size and must be planned, if appropriate. Communication should not only be about tasks to be achieved and planned but also any useful information to help comprehend them. HERMES also makes provision for a project marketing sub-model which deals with communication outside the project, including with the purchaser, users and operators.
11	Does the PM methodology call for identification of risks to individuals	HERMES makes clear provisions for a risk management sub-model. However, it is

	Touch points questions	Evidence from HERMES
	and to the organisation?	mainly geared towards the risks which could endanger the project's success and not the risks arising to individuals or to the organisation because of the project's negative impacts. Within the information security and data protection (ISDP) task, HERMES is more open to risks arising to individuals through the use of their personal data. In this regard, HERMES clearly calls for the use of data protection measures.
12	Does the PM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	Within its risk management sub-model, HERMES uses a full approach which includes: recognition of risks; analysis of risks (causes, effects); risk appraisal, with respect to their effects; reduction or, if possible, elimination of the risks; planning for the likelihood of residual risks; supervision of residual risks and of the effects of measures introduced; setting up reserves for residual risks. Moreover, all this analysis must be fully documented.
13	Does the PM methodology include provisions for documenting the process?	HERMES is a narrative project management method. All project requirements, specifications, organisation, objectives, expected results, etc. must be documented. And those documents must be kept up to date during the development cycle.
14	Does the PM methodology include provision for making the resulting document public (whether redacted or otherwise)?	HERMES includes a project marketing sub-model which handles all communication inside and outside the project. However, there is little or no evidence to suggest the release of documents to the wider public.
15	Does the PM methodology call for a review if there are any changes in the project?	As a process, HERMES calls for a continual update of the project's specifications with regard to expected results. If appropriate, any changes in the project must be synchronised with the quality assurance plan, then verification and audits must be run accordingly.
16	Does the PM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	HERMES features a quality management (QM) sub-model which is run throughout the project. This sub-model includes provisions for verification and audits to ensure that all of the specifications have been adequately taken into account, implemented and documented. However, unlike other methodologies, HERMES doesn't go beyond the deployment and finalisation phases. Hence, all of its requirements for verification and audit don't

	Touch points questions	Evidence from HERMES
		cover the production, maintenance and retirement phases.

Conclusions and recommendations

HERMES includes provisions for handling information security and data protection requirements set out in the Swiss Data Protection Act, which represents an important step for the inclusion of privacy impacts and privacy protection. However, regarding PIAs, HERMES lacks provisions for broad privacy protection and broad stakeholder involvement.

Nevertheless, as a results-oriented project management method, HERMES has some features which open doors for better integration with PIAs. One of those key features is Tailoring which brings together all necessary tools and rules to include new project-specific requirements and objectives. Tailoring starts at the beginning of a project and runs throughout all project phases. Tailoring should be seen as the first place to include the requirements for a broad privacy analysis as well as a wider consultation with more stakeholders than those directly involved in the project development.

The quality management sub-model provides the opportunity to take into account new requirements in terms of all the necessary verifications and audits to ensure appropriate privacy protection. The project marketing sub-model could be extended to carry out wider stakeholder communication and involvement. The risk management sub-model could also be extended to take into account not only those risks that could endanger the success of the project but also those that could arise due to possible negative impacts by the use of project production.

2.3 DERIVATIVE PM APPROACHES

Whilst these project management approaches are those with broad adoption, a key issue that should be considered is how to integrate PIAs into existing PM methodologies that are derivatives of these. Many large system integrators and technology service organisations use their own internal standards for project management, making the case to their clients for the added value of their "unique" methodologies. According to the 2012 PWC survey conducted across 38 countries with 1,524 respondents, 4% of organisations have developed their own in-house project management methodology.[77]

As an example, IBM Global Services, the IT consulting services arm of IBM with over 150,000 employees worldwide, requires its project managers to learn and apply its proprietary project management methodology. The methodology is largely based upon PMBOK, and as a matter of practice, professional project managers are typically also required to have a current PMP certification as a base of knowledge.[78]

Whilst it may not be viable to directly influence such proprietary approaches, education of working project managers as a part of an ongoing accreditation processes for the dominant PMBOK and PRINCE2 methodologies can provide a strong influence for change. In

[77] PriceWaterhouseCoopers, 2012.
[78] Interview on 13 March 2013 with IBM Global Services Project Manager, D. Tencza.

addition, where these standards are specifically being used by large global consultancies, there is an opportunity to impact many other organisations that engage their services, and look to them as models for good practice.

In addition, 8% of the responding organisations indicated that they used a combination of methodologies, while 26% indicated that they used none.

In those organisations where hybrid approaches are used, this is typically a reflection of trends towards integrating Agile methodologies within an organisation where traditional project management approaches have been used in the past, or that of integrating Agile into IT organisations where waterfall methodologies have been used. The project manager continues to play a role in maintaining traditional phase-based project management components in a majority of organisations where Agile is in place.[79] As organisations transition to Agile, they may perform some pilot projects applying an Agile methodology, while maintaining more traditional project and portfolio management approaches on a broad basis.

2.4 PRACTICAL APPROACHES FOR INTEGRATING PRIVACY RISKS INTO PROJECT MANAGEMENT STANDARDS AND METHODOLOGIES ADOPTED BY RESPONDENTS

The data collected through the January 2013 survey have been useful for identifying some of the potential "open doors" that some of the surveyed organisations are already using in order to integrate privacy risks into their project management processes and adopted standards. Rather than providing an exhaustive list of "open doors", this section summarises the most adopted "open doors" for integrating privacy risks into adopted project management standards, based on the responses received. This summary could provide useful directions for achieving practical integration.

Based on the responses, integration occurs, most of the time, at the project initiation phase, when the organisation needs to provide formal approval for, and finalise the scope and resources of the project. By taking the project life-cycle into consideration, we have organised the identified open doors around three main phases: *pre-project open doors*, *project-initiation open doors* and *project-implementation open doors*. The following is the list of identified open doors, as emerging from the survey, with a brief explanation for each of them.

Pre-project open doors

- *Procurement requisition process and documentation*: When raising a new procurement requisition, the project manager, responsible for opening the new requisition, needs to assess, by applying screening questions and/or a checklist, whether the new requisition involves privacy risks and therefore whether a PIA is required.
- *Service level agreement (SLA)*: When drafting a new service level agreement, the project manager in charge of the SLA has the responsibility to assess whether privacy risks are involved and if a PIA is required. For the assessment, the project manager could use a privacy screening checklist.

[79] PriceWaterhouseCoopers, 2012.

- *Business case process and documentation*: A few organisations have designed business case templates to contain a data protection compliance section requiring confirmation that the owner of the business case has consulted the information governance team in relation to privacy risks and has carried out an initial privacy assessment, often based on the privacy check list modelled on ICO guidance.
- *Review stage gate process*: This process refers to the critical management review stage gates where senior stakeholders (i.e., board) agree go or no-go decisions for the project. The review state gate process documentation comprises a section on privacy impact assessment at each stage of the process, including the first review stage when senior stakeholders have to take decisions on project funding and go-ahead.

Project initiation open doors

- *Regulatory gateway assessment*: Immediately after the project go-ahead, projects go for an internal regulatory assessment where, as one of the respondents has stated: they "are assessed to ascertain if Privacy is in scope. If in scope, the Project management team are required to fill in a PIA before the project can progress. From this, the Privacy team are able to advise on the level of involvement needed in the project to manage risk and compliance."
- *Information security assessment:* All of the projects, before initiation, have to go through an initial information security assessment, which includes an easy and simple privacy screening. If the security assessment, which is often done online, has highlighted information governance risks, including privacy, then the data protection office will provide information governance and privacy advice to the project manager at the inception of the project to properly identify, assess and manage potential impacts. Furthermore, organisations might issue internal information security guidance, including how to assess and manage privacy impact, to support project managers in their assessment.
- *Referral to an Information Security Forum (ISF):* At the project inception, project managers have to refer their projects to an Information Security Forum, which will initially assess information and privacy risk and advise the project manager on the necessary steps to take.
- *Project initiation documentation*: PIA is incorporated into the project initiation documentation in the form of an easy and quick initial privacy assessment. As one of the respondents has stressed: "The assessment of whether to undertake a risk assessment in relation to the need for a PIA is taken as part of the process of developing a Project Initiation Document". This is often done, within local authorities, in parallel with a risk assessment in relation to Equalities Impact Assessment (EqIA).[80]
- *Case for change management*: Some organisations have included PIA in the development of the case that project managers need to document, when project changes are requested. For any change management request, the project manager will assess the impact on privacy and the need for undertaking a PIA together with the assessment of other impacts, caused by the change request, such as cost, schedule, planned infrastructure, integration and input/output/processing modules.

[80] Introduced under the Equality Act 2010, Equality Impact Assessments are designed to protect the disadvantaged and the vulnerable. Under the act, public authorities have an equality duty. The duty is made up of a general equality duty supported by specific duties set out separately in the regulations. An equality impact assessment involves assessing the likely or actual effects of policies or services on people in respect of disability, gender and racial equality.

Project implementation open doors

- *PIA work-stream or work-package*: All large-scale projects have a formal privacy work- stream or work-package designed to monitor and manage privacy impact as the project progresses.
- *Review stage gate process:* This process refers to critical management review stage gates where senior stakeholders (e.g., board) agree go or no-go decisions for the project. The review state gate process documentation comprises a section on privacy impact assessment at each stage of the processes, including critical, intermediate phases of the project.
- *Project management toolkits:* The PIA process is formally integrated into a standard project management toolkit, which organisations use to manage projects.
- *Project Office's standards and methodologies:* PIA processes are fully integrated into the organisation's Project Office standards and methodologies and, therefore, consistently applied across the organisation.
- *Project management training:* Privacy and PIA training is incorporated into the organisation's standard project management training.

3 RISK MANAGEMENT STANDARDS AND METHODOLOGIES

This chapter parallels the previous chapter to some extent. It describes popular risk management standards and methodologies in use in the UK and abroad. The principal differences are that the risk management area is much more diverse in terms of available standards to be applied, and the scope of each differs.

For each methodology, we provide an overview followed by a table in which we "interrogate" the methodology using a set of questions derived from the PIA Handbook touch points. The following table, as with that in the introduction to Chapter 2, shows how we have converted the touch points into a set of questions.

	Touch points extracted from the ICO PIA Handbook	Questions for risk management methodology based on touch points
1	PIAs must comply with (more than just data protection) legislation. Private sector organisations will also have to consider industry standards, codes of conduct and privacy policy statements.	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?
2	PIA is a process.	Is the RM methodology regarded as a process or is it simply about producing a report?
3	A PIA could consider: 1. privacy of personal information; 2. privacy of the person; 3. privacy of personal behaviour; and 4. privacy of personal communications.	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?
4	PIA should be undertaken when it is possible to influence the development of a project.	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?
5	Responsibility for the PIA should rest at the senior executive level.	Does the RM methodology place responsibility for its use at the senior executive level?
6	The organisation should develop a plan for the PIA and its terms of reference. It should develop a consultation strategy appropriate to the scale, scope and nature of the project.	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?
7	A PIA should include an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources).	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?
8	The organisation should determine whether a small-scale or full-scale PIA is needed.	Does the RM methodology include provisions for scaling its application according to the scope of the project?
9	A PIA should seek out and engage	Does the RM methodology call for

	Touch points extracted from the ICO PIA Handbook	Questions for risk management methodology based on touch points
	stakeholders internal and external to the organisation. The assessor needs to make sure that there is sufficient diversity among those groups or individuals being consulted, to ensure that all relevant perspectives are represented, and all relevant information is gathered.	consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?
10	The organisation should put in place measures to achieve clear communications between senior management, the project team and representatives of, and advocates for, the various stakeholders.	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?
11	The PIA should identify risks to individuals and to the organisation.	Does the RM methodology call for identification of risks to individuals and to the organisation?
12	The organisation should identify less privacy-invasive alternatives. It should identify ways of avoiding or minimising the impacts on privacy or, where negative impacts are unavoidable, clarify the business need that justifies them.	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?
13	The organisation should document the PIA process and publish a report of its outcomes.	Does the RM methodology include provisions for documenting the process?
14	A PIA report should be written with the expectation that it will be published, or at least be widely distributed. The report should be provided to the various parties involved in the consultation. If information collected during the PIA process is commercially or security sensitive, it could be redacted or placed in confidential appendices, if justifiable.	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?
15	The PIA should be re-visited in each new project phase.	Does the RM methodology call for a review if there are any changes in the project?
16	A PIA should be subject to third-party review and audit, to ensure the organisation implements the PIA recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations.	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?

3.1 RISK MANAGEMENT

3.1.1 ISO 31000:2009 Risk management — Principles and guidelines

This International Standard provides the principles and guidelines for managing, systematically and transparently, any form of risk in any context.[81] A key feature of the standard is establishing the context in which the organisation operates. The context includes the organisation's objectives, its environment, and its stakeholders.

It recommends that organisations develop, implement and continuously improve a framework the purpose of which is to integrate the process for managing risk into the organisation's overall governance, strategy and planning, management, reporting processes, policies, values, and culture.

The standard comprises five main chapters on scope, terms and definitions, principles, framework, and process. It also has an annex on attributes of enhanced risk management and a bibliography.

Management of risk has numerous benefits. The standard points out that, among other things, it helps an organisation to

- identify opportunities and threats
- comply with legal and regulatory provisions
- improve stakeholder confidence and trust
- improve controls
- improve decision-making and planning
- improve organisational learning and resilience.

A good privacy impact assessment process has similar benefits.

The standard provides generic guidelines, but does not seek a uniform approach to risk management by all organisations.

Section 3 of the standard provides a set of risk management principles. Many PIA methodologies also contain a set of privacy principles. Among the principles in ISO 31000 is this one: Risk management is transparent and inclusive, i.e., the organisation should involve stakeholders in a timely manner. Including decision-makers from all levels of the organisation will help make sure that the organisation's risk management is current and relevant. Engaging stakeholders is the best way to ensure that their views are taken into account in identifying risks, setting risk criteria and finding solutions. Communication and consultation with stakeholders are also key features of PIA. Section 3 sets out 10 other principles as well.

Section 4 offers a framework for managing risk. It has several subsections which address:

[81] International Organization for Standardization (ISO), *Risk management – Principles and guidelines, ISO 31000:2009*, Geneva, 15 Nov 2009.

- The organisation's management and its commitment to the risk management policy, accountability and communicating with stakeholders
- Design of a framework for managing risk, which comprises tasks, including the following:
    - Understanding the organisation and its context
    - Establishing a risk management policy
    - Identifying who is accountable for managing risk(s)
    - Embedding risk management into organisational processes
    - Ensuring adequate resources are allocated for the risk management activities
    - Communicating with stakeholders, internal and external to the organisation
- Implementing the risk management framework
- Monitoring and reviewing the effectiveness of the framework.

The standard says that the effectiveness of risk management requires commitment by management, who should endorse the risk management policy, ensure the organisation complies with relevant legislation, assign responsibilities for managing and treating the risks, and communicate with all stakeholders.

The risk management process, the subject of section 5, includes these activities:

- Communication and consultation with internal and external stakeholders throughout the process – the organisation should consider different views when it defines risk criteria and evaluates risks. Communication and consultation are important because stakeholders make decisions based on their perceptions of risks, and those perceptions vary from one stakeholder to another.
- Establishing the context – the organisation needs to articulate the contextual factors that play a role in risk management. External factors include the legal and regulatory environment, the technological and competitive environment, etc. Internal factors include the organisation's objectives, strategy, structure, etc.
- Defining risk criteria, which include things like consequences, likelihood, level of risk, stakeholder views.
- Risk assessment comprises the following three activities:
    - Risk identification
    - Risk analysis, which means the organisation considers the sources of the risks, the consequences, the likelihood of the risks, the views of experts, uncertainties, availability of relevant information, the effectiveness of existing controls, etc.
    - Risk evaluation, which the organisation undertakes, using the risk criteria, to decide how to prioritise risks and to decide which need to be treated
- Risk treatment
    - Selection of risk treatment options, which include retaining, avoiding, reducing and sharing the risk(s).
    - Preparing and implementing risk treatment plans, which the organisation should discuss with relevant stakeholders
- Monitoring and review, the results of which the organisation should record and report externally and internally, as appropriate.
- Recording the risk management process, which provides a basis for improvement. There may be legal and regulatory requirements for such records.

	Touch point questions	Evidence from ISO 31000:2009
1	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	The standard says that understanding the external context includes understanding the legal and regulatory requirements.
2	Is the RM methodology regarded as a process or is it simply about producing a report?	Yes, the standard describes risk management as a process. Within that process, risk treatment is described as cyclical process of assessing the effectiveness of the way in which risks are treated.
3	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?	ISO 31000 is focused on risk management in a broad sense, so it does not focus particularly upon privacy protection. The word "privacy" does not appear in the standard. However, it does mention complying with laws and regulations, which would include privacy provisions.
4	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?	The standard says plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it.
5	Does the RM methodology place responsibility for its use at the senior executive level?	Effectively, yes. It says risk management requires commitment from the organisation's management, which should define and endorse its risk management policy and ensure there is accountability for managing risk.
6	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	The standard says the organisation should develop a plan for communicating and consulting with internal and external stakeholders, so that stakeholders understand the basis on which decisions are made, and the reason why particular actions are required.
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	Yes, understanding contextual factors figures prominently in the standard – both the external and internal context.
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	Not explicitly, but the standard does say that the organisation should define the criteria to be used to evaluate the significance of risk. When defining risk criteria, the organisation should take into account factors such as the following: • the causes and consequences and how they might be measured

	Touch point questions	Evidence from ISO 31000:2009
		• how likely the risks are • the timeframe of the likelihood and/or consequences • how the level of risk is to be determined • the views of stakeholders • the level at which risk becomes acceptable • combination of risks.
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	Yes, the standard says that communication and consultation with external and internal stakeholders should take place during all stages of the risk management process. It also says that if risk treatment options impact stakeholders, they should be involved in the decision-making process.
10	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	The standard says the organisation should establish internal and external communication and reporting mechanisms.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	ISO 31000 is focused on risks to the organisation, but it does say that perceptions of risk can vary due to differences in values, needs, assumptions and concerns of stakeholders.
12	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	Yes. Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, while taking into account legal, regulatory and other requirements such as social responsibility and the protection of the environment. Decisions should also take into account risks that can warrant risk treatment that is not justifiable on economic grounds; for example, where a risk could have severe consequences, but its likelihood is rare.
13	Does the RM methodology include provisions for documenting the process?	Yes, section 5.6 calls for monitoring and reviewing the risks and their treatment, while section 5.7 calls for recording the risk management process from beginning to end.
14	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?	Yes, in section 5.6 on monitoring and reviewing, the standard says the results should be recorded and reported externally and internally "as appropriate".
15	Does the RM methodology call for a review if there are any changes in the project?	Yes. The monitoring and review activity should include identifying emerging risks as well as any changes to the internal and external context, or to the risk criteria, or to

	Touch point questions	Evidence from ISO 31000:2009
		the risk itself.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	The standard does not use the word "audit", but, as mentioned above, the standard makes provision for monitoring and review; however, it does not explicitly provide for third-party review, other than potentially reporting to stakeholders "as appropriate".

Conclusions and recommendations

ISO 31000 appears to be the most prevalent risk management methodology. It shares some touch points with PIA, but because it is a generic risk management methodology, it does not address some PIA issues – for example, it does not use the word "privacy", nor is there any provision that might suggest recognition of data protection risks. However, communication and consultation with stakeholders are integral to the risk management process; hence, there are some "open doors" in the process where a PIA could be conducted. There is nothing in the standard that would be at odds with a PIA. ISO standards are revised from time to time. For example, the 27005:2008 standard was revised with a second edition in 2011. The same might happen with regard to 31000. If so, the ICO could urge the BSI (as an ISO member) to make more explicit potential risks to privacy and data protection. The existence of ISO 29100, which addresses privacy principles, is helpful in this regard.

3.1.2 Combined Code and Turnbull Guidance

The UK Corporate Governance Code 2010 is a set of principles of good corporate governance aimed at companies listed on the London Stock Exchange (LSE). It is overseen by the Financial Reporting Council (FRC), the UK's independent regulator responsible for promoting high quality corporate governance and reporting. The Financial Services Authority's Listing Rules have statutory authority under the Financial Services and Markets Act 2000. The Listing Rules require that companies listed on the stock exchange disclose how they have complied with the Code, and explain where they have not applied the code – in what the Code refers to as "comply or explain". The Code adopts a principles-based approach in the sense that it provides general guidelines of best practice. This contrasts with a rules-based approach to which companies must adhere.

The initial basis of the Code was the Cadbury Report, published in 1992, which was produced by a committee chaired by Sir Adrian Cadbury. That report covered financial, auditing, and corporate governance issues and made various recommendations, one of which was that each board should have an audit committee composed of non-executive directors. In 1994, the Cadbury Report principles were appended to the Listing Rules of the London Stock Exchange.

In 1996, a committee led by Marks & Spencer chairman Sir Richard Greenbury produced a report on executive compensation. The Greenbury Report also recommended some further changes to the existing principles in the Cadbury Code. In 1998, Sir Ronald Hampel, chairman and managing director of ICI plc, led a third committee, which published the Hampel Report; this suggested that the Cadbury and Greenbury principles be consolidated into a "Combined Code".

In 1999 came the first edition of the Turnbull guidance, which recommended that directors be responsible for internal financial and auditing controls. A committee, led by Nigel Turnbull of the Rank Group, prepared the Turnbull guidance, officially known as Internal Control: Guidance for Directors on the Combined Code. The Turnbull guidance was revised in 2005.[82]

In 2010, the Financial Reporting Council issued a new Stewardship Code, along with a new version of the UK Corporate Governance Code, thus separating the issues from one another.[83]

The Turnbull guidance is relatively short at 15 pages. It has five chapters – an Introduction, and chapters on maintaining a sound system of internal control, reviewing the effectiveness of internal control, the board's statement on internal control, and an appendix. The document provides guidance on the responsibilities of the board with regard to risk management, and on the responsibilities of the company to the board.

A preface states that the Financial Reporting Council asked a group to review the impact of the Turnbull Guidance produced in 1999. The group reported that boards and investors said the guidance had contributed to an overall improvement in risk management and internal control. "Notably, the evidence gathered by the Review Group demonstrated that respondents considered that the substantial improvements in internal control instigated by application of the Turnbull guidance have been achieved without the need for detailed prescription as to how to implement the guidance." In other words, companies preferred a principles-based approach to a rules-based approach, a preference that the review group endorsed. The group made only a small number of changes to the 1999 first edition of the Turnbull guidance.

The 2005 report emphasises that an effective system of internal control is not a one-off exercise: companies must take account of new and emerging risks, the assessment of which must be regular and systematic. The board is responsible for embedding risk management and control systems in their companies. The principal means of communication between the board, the company and shareholders is the annual report. The review group recommended that boards review whether they could make better use of the internal control statement in the annual report. "The internal control statement provides an opportunity for the board to help shareholders understand the risk and control issues facing the company". The review group says the board's attitude, reflected in that statement, is important for investors in deciding whether to invest in the company.

The Introduction to the 2005 report highlights the important of internal control and risk management. It notes that a company's objectives, internal organisation and the environment in which it operates are continually evolving and, as a result, so are the risks. Thus, internal control relies on "a thorough and regular evaluation of the nature and extent of the risks to which a company is exposed". Risks should not always be seen in a negative light; as this review points out, some risks present opportunities: "Since profits are, in part, the reward for successful risk-taking in business, the purpose of internal control is to help manage and control risk appropriately rather than to eliminate it." The point is repeated in para. 35.

---

[82] Financial Reporting Council, *Internal Control: Revised Guidance for Directors on the Combined Code* ["the Turnbull Guidance"], London, October 2005. © Financial Reporting Council (FRC). Adapted and reproduced with the kind permission of the Financial Reporting Council. All rights reserved. For further information, please visit www.frc.org.uk or call +44 (0)20 7492 2300.

[83] The above paragraphs are paraphrases extracted from http://en.wikipedia.org/wiki/Combined_code.

The guidance says that companies should incorporate risk management and internal control within their normal management and governance processes, and not as separate exercises to meet regulatory requirements.

The guidance quotes Principle C.2 of the Combined Code, which states that "The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets." It also quotes Provision C.2.1, which states that "The directors should, at least annually, conduct a review of the effectiveness of the group's system of internal control and should report to shareholders that they have done so."

Chapter two, on maintaining a sound system of internal control, says the board is responsible for setting policies on internal control and for making sure the internal control system is effective in managing risks. The board's deliberations should include a discussion of the nature and extent of risks facing the company, the extent to which the company can bear such risks, the likelihood of the risks, the company's resilience (i.e., its ability to reduce the incidence and impact of risks that materialise), and the cost/benefit of controls.

Management should identify and evaluate the risks faced by the company for consideration by the board and design, operate and monitor a suitable system of internal control that implements the policies on risk and control adopted by the board. Internal control of risks should be embedded throughout the company. All employees should have an understanding of the company, its objectives, the markets in which it operates, and the risks it faces; they should, accordingly, have some responsibility for internal control.

The guidance outlines the elements of an internal control system, which comprise policies, processes, tasks, behaviour and other aspects that enable it to respond effectively and quickly to business, operational, financial, compliance and other risks. The system will help to ensure internal and external reporting (which includes the maintenance of proper records that generate reliable information from within and outside the organisation) and compliance with applicable laws and regulations, as well as with internal policies.

The guidance emphasises that while it can help provide effective risk management, an internal control system cannot provide certainty against a company's risks.

Chapter three is on reviewing the effectiveness of internal control, which the guidance describes as an essential part of the board's responsibilities. In its decision-making, the board needs to take into account the scale, diversity and complexity of the company's operations and the nature of significant risks faced by the company.

An effective control system requires continual monitoring. The company should regularly provide the board with reports on internal control. The board should undertake an annual assessment in advance of making its public statement on internal control. Management reports to the board should provide "a balanced assessment" of the significant risks and the effectiveness of the system of internal control in managing those risks. Management should identify any significant failings or weaknesses in the reports as well as what actions it is taking to overcome them. The guidance says it is essential that management be open in its communication with the board regarding risk and control.

For its part, the board should consider the significant risks and how the company has identified and evaluated and is managing them. It should assess the effectiveness of the internal control system and whether more extensive monitoring is needed. The board should assess the scope and quality of management's risk monitoring, its internal control and audit, the extent and frequency of management's communication with the board as well as the effectiveness of the company's public reporting processes.

Chapter four concerns the board's statement on internal control. Paragraph 33 says the annual report and accounts "should include such meaningful information as the board considers necessary to assist shareholders' understanding of the company's risk management processes and system of internal control, and should not give a misleading impression". Paragraph 34 says the board should disclose (if it is true, of course) that there is an ongoing process for identifying, evaluating and managing the significant risks faced by the company, and that it is regularly reviewed by the board. Paragraph 37 reminds us that the Listing Rules require the board to disclose if it has failed to conduct a review of the effectiveness of the company's internal control system.

Chapter five is an appendix, which contains some questions to help the board to assess the effectiveness of the company's risk and control processes. For example, regarding risk assessment, the guidance asks if the company has communicated clearly with employees on risk assessment and internal control issues. Are significant risks identified and assessed on an ongoing basis? Regarding control, it asks whether senior management demonstrates commitment to fostering a climate of trust and integrity within the company. Regarding information and communication, it asks if management and the board receive timely, relevant and reliable reports on risks and information from inside and outside the company that are needed for decision-making. It asks: Are half-yearly and annual reporting effective in communicating a balanced and understandable account of the company's position and prospects? Are there established channels of communication for individuals to report suspected breaches of law or regulations or other improprieties?

It also asks if there are ongoing processes embedded within the company for monitoring and re-evaluating risks, policies, processes, and activities for risk management and internal control. It says such processes may include codes of conduct and/or internal audits. It asks whether management communicates with the board on the effectiveness of ongoing monitoring process regarding risk and control.

	Touch point questions	**Evidence from the Combined Code and Turnbull Guidance**
1	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	The Turnbull guidance does not specify particular legislation, but it does say that a sound system of internal control helps ensure compliance with applicable laws and regulations as well as internal policies.
2	Is the RM methodology regarded as a process or is it simply about producing a report?	The guidance says an effective internal control system should involve processes for monitoring the continuing effectiveness of the system of internal control (Chapter 2).
3	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?	It does not specifically mention privacy matters, but presumably privacy risks would be considered within its wider consideration

	Touch point questions	Evidence from the Combined Code and Turnbull Guidance
		of risks.
4	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?	The guidance sees risk management and internal control as a continual process, and says that management should report to the board on how it has addressed or is addressing risks.
5	Does the RM methodology place responsibility for its use at the senior executive level?	Yes, but it says that risk management and control should be embedded within the company and that all employees have some responsibility regarding risk management and control.
6	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	The guidance does not use the term "consultation", but it does refer to communication between management and the board, as well as to internal and external reporting.
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	Yes. It says (in the Preface) that no control system can be effective unless it takes account of the company's circumstances.
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	Not specifically.
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	No. There is a difference between stakeholders and shareholders.
10	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	Chapter 2 (para. 19) of the Turnbull guidance concerns the quality of internal and external reporting and a flow of timely, relevant and reliable information from within and outside the organisation. The board should make at least an annual public statement on the company's internal control (i.e., as part of the annual report). Paragraph 31 also refers to the effectiveness of the company's public reporting processes.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	No, only to the company.
12	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative	Yes.

	Touch point questions	Evidence from the Combined Code and Turnbull Guidance
	impacts are unavoidable, does it require justification of the business need for them?	
13	Does the RM methodology include provisions for documenting the process?	Yes.
14	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?	Yes, in some form. In Chapter five, it asks about senior management fostering a climate of trust.
15	Does the RM methodology call for a review if there are any changes in the project?	Yes. It sees risk management and internal control as an ongoing process.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	The guidance assumes that a company has an internal audit function (see, for example, clause 31).

Conclusions and recommendations

The Turnbull guidance is not a methodology, as, for example, ISO 31000 is, but it is important because it does provide a risk-based guidance for listed companies. We assume that, for listed companies, it is the most important risk guidance. It does not refer to other methodologies, such as ISO 31000 or ISO 27005, and says nothing about engaging stakeholders (shareholders are stakeholders, but not all stakeholders are shareholders), although it does refer to communication with shareholders and investors, and to fostering a climate of trust and integrity. From a review of touch points above, we can see some comparability between PIA and the Turnbull guidance. The ICO could communicate with the Financial Reporting Council and see whether there might be a possibility for strengthening the Turnbull guidance and/or the UK Corporate Governance Code with more specific provisions regarding privacy risks, and with encouraging companies to undertake a PIA to identify and respond to privacy risks. In any event, if the proposed Data Protection Regulation comes into force with Article 33 more or less intact, companies will be obliged to undertake PIAs. Thus the ICO could brief the Financial Reporting Council on the efficacy of PIA. It could cite the DECC PIA as an example of a relatively good PIA, and note that the Energy Networks Association undertook it in order to foster trust and transparency with consumers. Similarly, the ICO could point to other companies who undertake PIAs (such as Vodafone, Siemens and Nokia) and to the importance these companies attach to their reputation as a core corporate asset.

3.1.3 UK Treasury's The Orange Book: Management of Risk

The UK Treasury's *The Orange Book: Management of Risk – Principles and Concepts* (2004) is not untypical in seeing the identification, assessment, addressing and reviewing/reporting risks as (non-linear) steps in the risk management process. It identifies protection of privacy

as one of several operational risks to an organisation's information resources. Its employment of the concept of "risk appetite" (the amount of risk that is considered to be tolerable and justifiable) and its addressing of risk through an analysis of preventive and corrective controls seem in principle to provide an avenue for considering privacy impact, although privacy is not dealt with in *The Orange Book*.

The *Orange Book* is a relatively short document that succeeds a 2001 *Orange Book* "that proved very popular as a resource for developing and implementing risk management processes in government organisations". It reflects lessons learnt in the previous three years and is designed to be read in conjunction with a range of other central-government risk-management materials. It notes that, now that basic risk management is in place in the central public sector, attention is turning to continuing review and improvement. Observing that there is no specific standard for risk management in government organisations, the *Orange Book* aims to establish principles and a "Risk Management Assessment Framework". It leaves it to organisations to adopt specific standards, including Australian and Canadian ones. The *Orange Book* identifies the need for integrating risk management at strategic, programme and operational levels, led from the top, and with each organisation having a risk management strategy. It therefore sets out a "risk management model", emphasising the non-linear nature of a process that balances interwoven elements, that is sensitive to the way the management of one risk may have an impact on another one, and that places risk management in context.

The core process consists of four (non-linear) stages:

- identifying risks,
- assessing risks,
- addressing risks,
- reviewing and reporting risks.

The "extended enterprise", or organisational context for an organisation's risk management, has three elements:

- partner organisations,
- sponsored/sponsoring organisations,
- other government departments.

The risk environment or context identifies seven diverse elements:

- government,
- Parliament,
- stakeholder expectations,
- corporate governance requirements,
- the economy,
- capacity,
- laws and regulations.

The identification of stakeholder expectations and of relevant laws and regulations would be congruent with PIA if information and privacy risk were identified as foci for analysis.

The stage of *identifying risk* is the first step, which has two distinct phases: initial risk identification, and continuous risk identification. Both of these relate risks to objectives. Risks may be identified either through commissioning a risk review and/or by internal self-assessment in each level or part of the organisation. Risks are not independent of each other,

but may form groupings. Furthermore, identified risks should be assigned to an owner for management and monitoring. Horizon-scanning is highlighted as being of importance. The *Orange Book* provides an exemplary table showing typical groupings and sources of risk in a "PESTLE" model of external risks: political, economic, sociocultural, technological, legal/regulatory, and environmental. We may note that the legal/regulatory category mentions "EU requirements/laws which impose requirements (such as Health and Safety or employment legislation)"; it is likely that EU and UK requirements for data protection, and for PIA, would fall into this category and thus enter into the *Orange Book*'s risk management cycle as a "touch point".

The same table itemises a range of "operational risks" that includes main headings of:

- delivery,
- capacity and capability,
- risk management performance and capability.

Among these items are compliance with relevant requirements, ethical considerations, information security, accountability (to Parliament), and the resilience of IT to threats; it could be supposed that any of these might serve as a trigger for PIA.

It also mentions several "change risks", or risks "created by decisions to pursue new endeavours":

- PSA targets,
- change programmes,
- new projects,
- new policies.

It could be argued that, where such changes potentially involve new information-processing infrastructures and requirements, the need for PIA could correspondingly be identified within a privacy risk management routine.

The stage of *assessing risks* emphasises the need to assess both the likelihood and the impact of any risk, to record the assessment in a way that facilitates monitoring and the identification of priorities, and to be clear about how inherent and residual risk differ. Risk assessment can be either numerical or subjective depending on the kind of risk involved. A heuristic, simple matrix is shown for displaying likelihood and impact, with possible categorisations of "high/medium/low" – a 3x3 matrix, although 5x5 would be possible where risks are quantifiable. The tolerability of a risk is judged against the concept of "risk appetite", which is described more fully later in the *Orange Book.* Risks before controls are applied are inherent; those that remain after controls are residual. Both kinds are assessed against risk-tolerability levels.

The *Orange Book* emphasis on the need for full documentation of the stages in the process of risk assessment, thus creating a risk profile, facilitates not only the management of risk in all its phases but also, it would seem, aids transparency and accountability, which are also essential elements of PIA.

"Risk appetite" has to do with "the level of exposure which is considered tolerable and justifiable should [the risk] be realised". It is related to a benefit/loss calculation for the organisation faced with constraining the risk. The *Orange Book* further analyses risk appetite in three dimensions:

- corporate risk appetite [at the overall level of the organisation],
- delegated risk appetite [at cascaded lower levels, each of which may have different appetite levels],
- project risk appetite [at the project level].

Addressing risks "turn[s] uncertainty to the organisation's benefit by constraining threats ad taking advantage of opportunities" by pointing towards action to be taken ("internal control"). The *Orange Book* delineates five key aspects, or possible decisions once risks are assessed:

- tolerate,
- treat,
- transfer,
- terminate,
- take the opportunity.

Most risks will be treated, for which there are four different types of control:

- preventive controls,
- corrective controls,
- directive controls,
- detective controls.

In one way or another, these run the gamut from precautionary to remedial approaches to risk. Because "the purpose of control is to constrain risk rather than to eliminate it", the guiding principle is *proportionality*. We can note that PIA likewise requires action to be taken to mitigate diagnosed privacy risk, either in terms of elimination or minimisation, and with reasons given; this seems compatible with *Orange Book* requirements.

Reviewing and reporting risks is a crucial stage in risk management for the purpose of monitoring any change in the risk profile, and for gaining assurance about the effectiveness of the risk management; this is similar to PIA's revisitation in each project phase. As far as reporting is concerned, the *Orange Book* invokes several techniques to achieve review:

- risk self-assessment [at any level],
- "stewardship reporting" [upward accountability],
- the "Risk Management Assessment Framework" [Treasury].

Internal audit and the possible appointment of a Risk Committee are indicated as important in this stage.

Cutting across all the sages is *communication and learning*, both within the organisation and with external partners and stakeholders. Because no organisation is independent, the "extended enterprise" impinges on the organisation's risk assessment processes and risks arising in those relationships will also need to be managed. Finally, the context (see above), including stakeholders' expectations as well as laws and regulations, has to be taken into account in the formal risk management process cycle. Appendices in the *Orange Book* give further elaboration of *assurance principles*, emphasising matters to do with the nature of evidence and its evaluation in the risk-management process.

	Touch point questions	**Evidence from the *Orange Book***
1	Does the RM methodology include provisions about compliance with	The *Orange Book* is for public-sector organisations, but they must comply with

	Touch point questions	Evidence from the *Orange Book*
	legislation and any relevant industry standards, code of conduct, internal policy, etc.?	legislation, as the risk management process clearly indicates.
2	Is the RM methodology regarded as a process or is it simply about producing a report?	The *Orange Book* delineates a process but not with any PIA reference.
3	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?	No types of privacy are addressed.
4	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?	This could be adaptable to the *Orange Book* process, especially where changes (see this report) have resulted in new information projects amenable to PIA.
5	Does the RM methodology place responsibility for its use at the senior executive level?	The *Orange Book* puts responsibility of various kinds at relevant levels.
6	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	The *Orange Book* risk assessment approach, with its various steps, does this although not specifically in terms of a plan, even less in terms of a consultation strategy, and not with regard to any PIA, although this would seem compatible.
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	Not in these terms. The *Orange Book* risk - assessment approach scans the environment and the horizon, but not with regard to any PIA, although this would seem compatible.
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	The *Orange Book* does not do this, but (as argued in this report) this could plausibly be done, partly because the risk assessment cycle includes different levels of risk and levels of risk tolerability to which PIAs of different scales could be tailored.
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	The *Orange Book* says that the risk assessment should consider the perspectives of the whole range of stakeholders affected by the risk. It is also explicit in terms of relationships with the "extended enterprise" and the external, contextual environment.
10	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	Excepting the stakeholders (who, however, are highlighted in terms of communication), the *Orange Book* concentrates on relations and communication at all levels within the organisation.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	Risk to the organisation is the paramount concern, but risk to individuals (or to the privacy of outsiders) is not mentioned.
12	Does the RM methodology include	Protection measures form part of the

	Touch point questions	Evidence from the *Orange Book*
	provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	"proportionality" element and of the idea of containing risk.
13	Does the RM methodology include provisions for documenting the process?	Documentation is emphasised.
14	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?	Publication is not explicitly mentioned although communication with outsiders is seen as important.
15	Does the RM methodology call for a review if there are any changes in the project?	The *Orange Book* embeds this in one stage.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	The *Orange Book* emphasises both of these, but perhaps not so explicitly in terms of implementation.

Conclusions and recommendations

Although the *Orange Book* does not engage with privacy or with risk to individuals, it is likely that EU and UK requirements for data protection, and for PIA – as laws that create requirements – would enter into the *Orange Book*'s risk management cycle as a "touch point". If so, this could provide an "open door" for PIA. Many of the points in its risk management methodology seem compatible with PIA, and the way it addresses risk through an analysis of preventive and corrective controls could also provide a gateway for considering privacy impact as part of a mitigating strategy. So, too, could the *Orange Book*'s concern with stakeholder expectations. Its discussion of potential risks brought about by new projects could also provide an "open door" if such projects involved new IT projects and systems, for which the need for PIA could be identified within a privacy risk management routine.

3.1.4 ENISA's approach to risk management

ENISA defines risk management as the process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options. ENISA's approach to risk management is detailed in the first 38 pages of a 168-page report, the remainder of which is an extensive inventory of other risk management methods and tools.[84] The first nine chapters are: Introduction; Structure and target groups of this document;

[84] European Network and Information Security Agency (ENISA), *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools*, Heraklion, June 2006. http://www.enisa.europa.eu/activities/risk-management

Positioning risk management and risk assessment; Risk management processes; The corporate risk management strategy; Risk assessment; Risk treatment; Risk acceptance; and Monitor and review. Chapter 12 provides a road map for current and future trends in risk management.

For ENISA, the risk manager must strike a balance between realising opportunities for gains and minimising vulnerabilities and losses. Risk management should be part of good corporate governance and an endlessly recurring process. In positioning risk management and risk assessment, ENISA says its approach is based on OCTAVE and ISO 13335-2 (which became ISO 27005). It says risk assessment is part of the risk management process, which deals with analysis, planning, implementation, control and monitoring of implemented measurements, and enforcement of the organisation's security policy. By contrast, risk assessment is executed at specific points (e.g., once a year, on demand, etc.) and – until the performance of the next assessment – provides a temporary view of assessed risks while setting parameters for the entire risk management process.

It notes that there are various standards and good practices in risk management and risk assessment, as its annexes make clear, but that organisations, in practice, tend to adapt these to their own needs, which helps to create good practices for particular sectors. While organisations tend to adopt a single risk management method, different risk assessment methods might be necessary, depending on the nature of the assessed system (e.g., structure, criticality, complexity, importance, etc.).

ENISA discusses risk management within an Information Security Management System (ISMS), wherein it states that security depends on people more than on technology, that employees are a far greater threat to information security than outsiders, and that the degree of security depends on three factors: the risk you are willing to take, the functionality of the system and the costs you are prepared to pay. It notes that information confidentiality, integrity and availability requirements have implications for business continuity, minimisation of damages and losses, competitive edge, profitability and cash-flow, the organisation's image, and legal compliance.

ENISA lists several critical success factors for ISMS. Among them, to be effective, the ISMS must:

- have the continuous, visible support and commitment of the organisation's top management,
- be an integral part of the overall management of the organisation,
- be based on continuous training and awareness of staff and avoid the use of disciplinary measures and "police" or "military" practices,
- be a never-ending process.

Large organisations address information security for various reasons, notably their legal and regulatory requirements that aim at protecting sensitive or personal data as well as general public.

The ENISA document sets out six key steps in the development of an ISMS framework:

1. Definition of security policy
2. Definition of ISMS scope
3. Risk assessment (as part of risk management)
4. Risk management
5. Selection of appropriate controls and

6. Statement of applicability.

Step 6 documents the risks facing the organisation and the security controls the organisation could deploy. Chapter 4 on risk management processes says the effectiveness of RM depends on the degree to which it becomes part of an organisation's culture, its practices and business processes. Risk management should be the responsibility of everyone in the organisation. ENISA distinguishes between the management of known risks and of emerging risks. Risk management, as described in this document, addresses known risks, while emerging risks are addressed via scenarios.[85]

It says its risk management process provides for interfaces to other operational and product processes. Ideally, it says, risk management should start with the establishment of a corporate risk management strategy, then proceed to risk assessment, risk treatment, monitoring and review and feed back into the strategy. Risk communication and awareness should permeate the process, which should interface to other operational and product processes. It makes the point that an effective risk management system must have such interfaces.

Risk assessment comprises three steps: risk identification, analysis and evaluation. Risk treatment is the process of selecting and implementing measures to modify risk. Its measures include avoiding, optimising, transferring or retaining risk. Risk communication is defined as "a process to exchange or share information about risk between the decision-maker and other stakeholders inside and outside an organization". ENISA describes monitoring and reviewing as a "process for measuring the efficiency and effectiveness of the organization's RM processes. This process makes sure that the specified management action plans remain relevant and updated. This process also implements control activities including re-evaluation of the scope and compliance with decisions."

Chapter 5 focuses on corporate risk management strategy, which is described as an integrated business process incorporating all of the risk management processes, activities, methodologies and policies adopted and carried out in an organisation. It consists of two processes, one setting the framework for the entire risk management and the other setting the communication channels in the organisation.

Risk communication, it argues, should involve an open discussion with all stakeholders aimed at the development of a common understanding, rather than a one-way flow of information from the decision-maker to other stakeholders. Risk management will be enhanced if stakeholders understand each other's perspectives and if they are consulted in a timely fashion. Stakeholders, like all human beings, tend to make judgements about risk based on their perceptions. These can vary due to differences in values, needs, assumptions, concepts and concerns. Thus, the organisation should identify, evaluate and take into account variations in the values held and the perceptions of risk of the various stakeholders in the decision-making process. ENISA encourages organisations to plan and implement external communications and consultation on a regular basis. External stakeholders, it says, bring in "fresh air" with their additional viewpoints in the evaluation of risks.

ENISA focuses on the organisation's establishing a risk management framework, which should help the organisation to clarify and to gain a common understanding of its objectives,

[85] ENISA, *EFR Framework: Introductory Manual*, March 2010. http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/emerging-and-future-risks-framework-introductory-manual.

to identify the environment in which it operates, and to develop the criteria against which risks will be measured.

The external environment typically includes:
- the local market, the business, competitive, financial and political environment
- the law and regulatory environment
- social and cultural conditions
- external stakeholders.

The risk manager should also have a good understanding of the organisation's internal environment which includes:
- key business drivers (e.g., market indicators, competitive advances, product attractiveness, etc.)
- the organisation's strengths, weaknesses, opportunities and threats (the familiar "SWOT")
- internal stakeholders
- organisation structure and culture
- assets (such as people, systems, processes, capital, etc.)
- goals and objectives and the strategies to achieve them.

After developing an understanding of the external and internal context, the risk manager can generate a risk management context, which involves defining:
- the organisation, process, project or activity (to be assessed) and establishing its goals and objectives
- the duration of the project, activity or function
- the scope of the risk management activities to be undertaken
- the roles and responsibilities of those participating in the risk management process
- the dependencies between the project or activity and other projects or parts of the organisation.

Chapter 5 also has a section on the criteria by which risks will be evaluated. The organisation has to agree the criteria for deciding whether risk treatment is required, which is usually based on operational, technical, financial, regulatory, legal, social, or environmental criteria, or on combinations of them. Risk criteria could include:
- impact criteria and the kinds of consequences that will be considered
- criteria of likelihood
- the rules that will determine whether the risk level is such that further treatment activities are required.

Chapter 6 is on risk assessment. It points out that every organisation is continuously exposed to new or changing threats and vulnerabilities. The organisation should identify, analyse and evaluate the threats and vulnerabilities, measure the impact of the risk involved, and decide on the measures and controls to manage them.

In general, a risk can be related to or characterised by:
(a) its origin
(b) a certain activity, event or incident (i.e., threat)
(c) its consequences, results or impact
(d) a specific reason for its occurrence
(e) protective mechanisms and controls (or their lack of effectiveness)

(f) time and place of occurrence.

Identifying what may happen is rarely sufficient. The fact that there are many ways in which an event can occur makes it important to study all possible and significant causes and scenarios. Methods and tools used to identify risks and their occurrence include checklists, judgements based on experience and records, flow charts, brainstorming, systems analysis, scenario analysis, and systems engineering techniques.

Chapter 6 discusses risk analysis, the process whereby the risk manager attempts to assess and understand the level of the risk and its nature. Risk analysis involves:

- thorough examination of the risk sources
- their positive and negative consequences
- the likelihood that those consequences may occur and the factors that affect them
- assessment of any existing controls or processes that might minimise negative risks or enhance positive risks.

Risk analysis techniques include

- interviews with experts in the area of interest and questionnaires,
- use of existing models and simulations.

Risk analysis may vary in detail according to the risk, the purpose of the analysis, and the required protection level of the relevant information, data and resources. Analysis may be qualitative, semi-quantitative or quantitative, or a combination of these. A risk may have monetary, technical, operational and/or human consequences.

During the risk evaluation phase, the organisation must decide which risks to treat and which not to, and their priorities for treatment. Analysts need to compare the level of risk determined during the analysis process with the risk criteria, which should take into account organisational objectives, stakeholder views, and the scope and objective of the risk management process itself. The decisions made are usually based on the level of risk in terms of:

- consequences (e.g., impacts)
- the likelihood of events
- the cumulative impact of a series of events that could occur simultaneously.

Chapter 7 focuses on risk treatment, which is the process of selecting and implementing measures to treat risks. Treatment options are avoiding, optimising (or minimising or modifying), transferring (or sharing), or retaining risk. Not all risks carry the prospect of loss or damage, and some risks may present opportunities. The risk manager should compare the cost of managing a risk with the benefits obtained or expected. It is important to consider all direct and indirect costs and benefits, whether tangible or intangible, and measured in financial or other terms. Treatment plans should describe how the chosen options will be implemented and should provide all necessary information about:

- proposed actions, priorities or time plans
- resource requirements
- roles and responsibilities of all parties involved in the proposed actions
- performance measures
- reporting and monitoring requirements.

Action plans should be in line with the values and perceptions of all types of stakeholder (e.g., internal, outsourcing partner, customer, etc.). Effective communications with the various stakeholders will make it easier to obtain their consent and commitment to implementation. Top management support is critical throughout the entire risk management process. Thus, the risk manager should keep the organisation's senior management regularly informed and updated. The risk management plan should spell out how risk management is to be conducted and embedded in all of the organisation's business and policy development processes, and in its business and strategic planning, as well as other plans and processes such as asset management, audit, business continuity, environmental management, fraud control, human resources, investment and project management.

The board should define and document its policy for managing risk, which may include:

- the objectives and rationale for managing risk
- the links between the policy and the organisation's strategic plans
- the extent and types of risk the organisation will take and the ways it will balance threats and opportunities
- the processes to be used to manage risk
- accountabilities for managing particular risks
- details of the support and expertise available to assist those involved in managing risks
- a statement on how risk management performance will be measured and reported
- a commitment to the periodic review of the risk management system
- a statement of commitment to the policy by directors and the organisation's executive.

Publishing and communicating a policy statement like this demonstrates to internal and external stakeholders the board's commitment to risk management and specifies who is accountable for managing particular risks. Top management must identify and allocate the resources necessary for risk management. Residual risks should be documented and subjected to regular review. Risk acceptance concerns the communication of residual risks to the decision-makers. Once accepted, residual risks are considered as risks that the management of the organisation knowingly takes.

Chapter 9 is entitled Monitor and Review, and argues that one of the most critical factors affecting the efficiency and effectiveness of the organisation's risk management process is the establishment of an ongoing monitor and review process to make sure that the risk management plans are relevant and up-to-date. To make risk management a part of the organisation's culture and philosophy, the organisation must collect and document experience and knowledge through a consistent monitoring and review of events, treatment plans, results and all relevant records. Each stage of the risk management process must be recorded appropriately. Assumptions, methods, data sources, results and reasons for decisions should be recorded.

	Touch point questions	**Evidence from the ENISA risk management methodology**
1	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	Section 3 mentions (briefly) legal compliance. Section 1 recognises a need to integrate IT risk management and risk assessment with existing methods and standards in the areas of information technology and operational risks.
2	Is the RM methodology regarded as a	A process. There are frequent references to

	Touch point questions	Evidence from the ENISA risk management methodology
	process or is it simply about producing a report?	this.
3	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?	Section 3 mentions legal and regulatory requirements that aim at protecting sensitive or personal data. It does not mention other types of privacy.
4	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?	Implicitly, yes. It sees risk management as a never-ending process.
5	Does the RM methodology place responsibility for its use at the senior executive level?	Yes. Chapter 7, for example, says that top management support is critical throughout the entire risk management process.
6	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	It refers frequently to planning throughout the process. While it also refers to consultation with internal and external stakeholders, it is not so specific as to including a consultation strategy appropriate to the scale, scope and nature of the project.
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	Yes. Chapter 5 calls for definition of the internal and external environment.
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	Yes, to some extent. For example, Chapter 6 says risk analysis may vary in detail according to the risk, the purpose of the analysis, and the required protection level of the relevant information, data and resources.
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	Yes. See Chapter 5.
10	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	Yes. See Chapter 5.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	No. It is focused on risks to the organisation.
12	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative	Yes. Chapter 7 concerns risk treatment and includes a section on residual risks. Chapter 8 address risk acceptance, wherein it says that once accepted, residual risks are considered as risks that the management of

	Touch point questions	Evidence from the ENISA risk management methodology
	impacts are unavoidable, does it require justification of the business need for them?	the organisation knowingly takes.
13	Does the RM methodology include provisions for documenting the process?	Yes.
14	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?	Yes.
15	Does the RM methodology call for a review if there are any changes in the project?	Not specifically, but it says that the organisation should regularly review its risk management plan and risk treatment plan.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	No, third-party review or audit is not mentioned, but Chapter 9 concerns regular internal review of the risk management plan.

Conclusions and recommendations

The ENISA risk management methodology is, as it states, primarily based on OCTAVE and the ISO 13395 standard (which became ISO 27005). It meets many of the "touch points". We can also identify several "open doors" (or interfaces) for integration of its risk management methodology with other corporate operational processes. Its inventory of other risk management methodologies makes it unique, among all of the reports we have examined, even though its review primarily consists of "tombstone" (basic) information with minimal descriptive content. Also of interest is ENISA's distinction between existing and emerging risks, and its approach to each. It manages existing risks using a somewhat tried and tested (but traditional) risk management approach, whereas it uses relatively elaborate scenarios to explore emerging risks. We can certainly endorse ENISA's identified open doors and its use of scenarios.

3.2 INFORMATION SECURITY

3.2.1 ISO/IEC 27005:2011 Information security risk management

This standard, an update of the first edition issued in 2008, comprises 12 sections and seven annexes over 68 pages.[86] It provides guidance on information security risk management. It provides a set of definitions for terms such as consequence, control, event, external context, internal context. It is especially useful to the note differences between terms such as risk analysis, risk assessment and risk evaluation. Risk assessment, for examples, includes risk identification, analysis and evaluation.

[86] International Organization for Standardization (ISO), *Information technology – Security techniques – Information security risk management, ISO/IEC 27005:2011, Second edition*, Geneva, 1 June 2011.

Section 5 provides some background on information security risk management, which, according to the standard, should be an ongoing, iterative process, which examines the external and internal context (an environmental scan), assesses the risks, and makes recommendations on how to treat those risks. It says stakeholders should be consulted and kept informed with regard to decisions on how to treat risks. Employees should also be educated about the risks and how the organisation is dealing with them. In addition, the process should be documented.

Section 7 concerns the context. It says the organisation can select different risk management approaches, but whichever is chosen, it should include criteria relating to risk evaluation, impact and risk acceptance. The criteria for risk evaluation should include the strategic value of business information, legal and regulatory obligations, contractual requirements, confidentiality, operational importance, stakeholder views, and reputational issues. The organisation should develop impact criteria relating to the damage that could be wrought by an information security event. It should also develop criteria specifying its risk acceptance taking into account the organisation's objectives and stakeholder interests. The organisation should also identify relevant assets and take into consideration its strategy, business, functions, constraints, socio-cultural environment, etc. It should also describe the environment in which it operates, and should identify and analyse stakeholders as well as its relationship with them.

Section 8 addresses information security risk assessment, saying that the organisation should identify, describe and prioritise risks. To assess risks, the organisation must first identify and value its information assets, then identify threats and vulnerabilities, possible controls and the consequences; then it can rank the risks according its risk evaluation criteria. The purpose of risk identification is to determine what could happen to cause a potential loss, and where, how and why the loss might occur. Risks could originate from within the organisation as well as outside it.

The organisation needs to define its assets. An asset is anything that has value to an organisation, which it thus needs to protect. Assets can be valued by determining the cost of replacing the asset as well as the consequence on the business or organisation if the asset is damaged or compromised. The latter cost is usually higher than the replacement cost. Similarly, the organisation should identify a list of threats to those assets. Threats may be accidental or deliberate, of natural or human origin. They may originate from within the organisation or externally. Examples of threats can be found in an annex as well as in other threat catalogues.[87]

Having identified relevant threats, the organisation should identify controls (or counter-measures) against those threats as well as vulnerabilities. Threats exploit vulnerabilities to cause harm to the organisation and its assets. Vulnerabilities relate to the organisation itself, its management, employees, physical environment, hardware and software. A further annex contains a list of vulnerabilities. Next, the organisation should identify and examine the consequences of a threat exploiting a vulnerability. ISO 27005 describes this as an incident

[87] For example, OSA (Open Security Architecture) is developing a threat catalogue. See http://www.opensecurityarchitecture.org/cms/en/library/threat_catalogue. The German Federal Office for Information Security (BSI) has produced several iterations of threat catalogues. See https://www.bsi.bund.de/EN/Topics/ITGrundschutz/Download/download_node.html.

scenario. A consequence could be a loss of business, damage to reputation, undermining effectiveness, etc.

Risk analysis assigns values to the likelihood and the consequences of a risk. The analysis may be qualitative, quantitative or a combination of both. A qualitative risk analysis uses words like "low, medium and high" to describe the magnitude and likelihood of a risk materialising. Quantitative risk analysis assigns numerical values on a scale. ISO 27005 says that risk analysis is based on assessed consequences and likelihood, is a variation on the classic formula: risk = probability (likelihood) x consequence.[88] There are different types of consequence if an asset is compromised – cost, technical, human, time, etc. The organisation should also assess the likelihood of a consequence. It can consider cost benefit, stakeholder concerns and other variables. In evaluating risk, the organisation should evaluate the identified risks using the criteria for risk evaluation and acceptance which it had previously established. It will also need to take into account legal, regulatory and contractual requirements, if any.

Section 9 concerns information security risk treatment. It focuses on controls (counter-measures) to reduce, retain, avoid or share risks based on a risk treatment plan. The organisation should decide which of these four options is the best, taking into account its risk assessment as well as the expected cost and benefit. The four options are not mutually exclusive. A part of the risk treatment plan should prioritise the risks to be treated. In doing so, the organisation should consider how the risk is or will be perceived by the affected parties and the best ways to communicate with those affected stakeholders. The risk treatment plan should also determine which risks will be residual, i.e., will remain with the organisation. One of the four options is to reduce or modify a risk. In selecting controls, the organisation should also factor in various constraints such as time, financial, technical, operational, ethical, legal, personnel, etc. A second option is to retain the risk, especially if it meets the previously established risk acceptance criteria. The third option is to avoid the risk, for example, by not pursuing a particular activity or by changing the conditions under which the activity would be undertaken. The fourth option is to share the risk, e.g., by taking out insurance.

Section 10 addresses information security risk acceptance. The organisation should justify why it is accepting certain risks (e.g., the benefits are attractive or the costs of reducing or avoiding a risk are too high). Section 11 addresses information security risk communication and consultation. The organisation is counselled to consult and communicate with its stakeholders on how to manage risks. The organisation should provide stakeholders with relevant information, e.g., on the existence of the risks, their likelihood, consequences, treatment and acceptability. Communication is a two-way process. Stakeholder perceptions of a risk can vary and, as a result, they will likely have different views on the acceptability of a risk. Risk communication is important to:

- Collect risk information
- Inform stakeholders about its risk assessment and treatment plan
- Support decision-making
- Co-ordinate with others
- Raise awareness.

[88] See, for example:
http://www.hpa.org.uk/ProductsServices/ChemicalsPoisons/ChemicalRiskAssessment/RiskAssessment/

The organisation should view risk communication as an ongoing activity, both for "normal" communications and emergency or crisis communications.

Section 12 concerns information security risk monitoring and review. As risks change and evolve, the organisation is urged to monitor and review risks on an ongoing basis and, in doing so, to pay attention to (new) threats, vulnerabilities, probabilities and consequences. The organisation should also monitor new assets and any change in the value of existing assets. The process of information security risk management itself should also be reviewed and improved, whenever and wherever possible. The organisation should also monitor its legal and environment context, its competitors, its risk assessment approach and associated criteria regarding risk evaluation, impact, and acceptance.

As mentioned, ISO 27005 has several annexes. Annex A is on defining the scope and boundaries of the information security risk management process, which is divided into four parts concerning study of the organisation, constraints affecting the organisation, legislative and regulatory references, and list of constraints affecting the scope. Annex B concerns identification and valuation of assets, and impact assessment. It provides and categorises a list of typical assets, and sets out criteria that could be factored into asset valuation. It also identifies direct and indirect impacts of an information security incident. Annex C categorises and lists examples of typical threats, which could be accidental, deliberate or environmental in nature. Annex D categorises and lists examples of vulnerabilities and sets out methods for vulnerability assessment. Annex E sets out information security risk assessment approaches, starting with a high-level approach and followed by a detailed approach. It also sets out some worked examples of matrices for assigning values to assets, threats and vulnerabilities in order to arrive at measures of risk levels. Annex F lists constraints for risk modification. Finally, Annex G highlights the differences between ISO 27005: 2008 and the 2011 second edition.

	Touch point questions	Evidence from ISO 27005:2011
1	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	Yes. It frequently mentions the need to comply with legal and regulatory requirements.
2	Is the RM methodology regarded as a process or is it simply about producing a report?	Section 5 says specifically that information security risk management should be a continual process.
3	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?	ISO 27005 refers to personal information and privacy at several points. However, it does not distinguish between information privacy (data protection) and other types of privacy.
4	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?	No. The focus of ISO 27005 is on information security risk management, no matter whether it is applicable to existing or new information systems.
5	Does the RM methodology place responsibility for its use at the senior executive level?	To an extent. For example, it states that "The risk acceptance activity has to ensure residual risks are explicitly accepted by the managers of the organization." It also says that risks and their treatment should be

	Touch point questions	Evidence from ISO 27005:2011
		communicated to appropriate managers and operational staff.
6	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	Yes. Section 11 is entitled "Information security risk communication and consultation", although it focuses (well) on just risk communication, and makes no mention of consultation strategy or techniques.
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	Yes. Section 7 is devoted to "Context establishment".
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	Not directly, but it does say that the information security risk management process can be applied to the organisation as a whole, or any part thereof, or any information system, existing or planned.
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	Yes. See section 11, as mentioned above. See also section 7.4 concerning the organisation for information security risk management, where it refers to a function of the organisation being to identify and analyse stakeholders and to define the roles responsibilities of all parties both internal and external to the organisation.
10	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	Yes, to some extent, especially in section 11, as mentioned above. However, it is treated rather briefly.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	The focus is mainly on identification of risks to the organisation, but it does mention risks to personal information, which is regarded as a primary asset.
12	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	Yes. It includes provisions for identifying controls against risks and for justifying any residual risks (those retained by the organisation). It does not specifically identify controls in the same way that it has identified threats and vulnerabilities.
13	Does the RM methodology include provisions for documenting the process?	Yes, it says, "The detailed results of every activity of the information security risk management process and from the two decision points should be documented" (section 6, p. 9).
14	Does the RM methodology include	It does not discuss making the information

	Touch point questions	Evidence from ISO 27005:2011
	provision for making the resulting document public (whether redacted or otherwise)?	security risk management report public *per se*, but it does say that information about the risks and risk treatment plans should be shared with stakeholders. See section 11.
15	Does the RM methodology call for a review if there are any changes in the project?	Yes. Section 12 says the organisation should constantly monitor risks and the associated threats, vulnerabilities, likelihood and consequences.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	To some extent. It says that controls should be subject to an audit of their effectiveness. It does say that the organisation managers should explicitly identify residual risks. It also says that the decision-maker should justify any decision to override normal risk acceptance criteria.

Conclusions and recommendations

ISO 27005 has many "touch points" in common with the PIA Handbook, as indicated above. One can see several "open doors" too, i.e., points in the information security risk management process where it would be possible to insert the PIA process. It could be done during the environmental scan (context establishment) phase. It could be done as part of the risk identification process (common to both ISO 27005 and PIA). It could be done during the process of identifying controls (counter-measures) against the risks. It could also be done in preparing the risk treatment plan. These are all open doors where all or some part of the PIA process could be included in the information security risk management process as described in ISO 27005. The most appropriate part would be in identifying risks and, subsequently, controls.

3.2.2 IT-Grundschutz

IT-Grundschutz[89] stands for "Information Technology Baseline Protection". It was formally known as "IT-Baseline Protection Manual" when it was first released in 1994 by the Bundesamt für Sicherheit in der Informationstechnik (BSI),[90] which is the German Federal Agency for Security in Information Technology. At that time, IT-Grundschutz was one document of thousands of pages[91] containing a set of recommended and proven standard security measures or safeguards for typical IT systems. Since 2005, along with regular updates, this document has been hugely restructured and split into three main documents (IT-Grundschutz Catalogue, IT-Grundschutz Methodology and Risk analysis based on IT-Grundschutz) while the general approach has shifted from IT security to information security in an attempt to align with current international standards (mainly the ISO 2700x family). All these documents are freely available in both German and English. However, the English translation is not as up to date as the documents in German.

[89] https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzHome/itgrundschutzhome_node.html
[90] https://www.bsi.bund.de/EN/Home/home_node.html
[91] The English version published in 2000 has 1,680 pages.
http://www.iwar.org.uk/comsec/resources/standards/germany/itbpm.pdf

IT-Grundschutz is a dedicated risk management methodology for information technology (IT) security as well as information security that can be easily used whatever is the situation of a specific organisation in the public or private sector. As such, one of its objectives is to provide "a pragmatic and effective approach to achieve a normal security level" by reducing "the expense of the information security process" with the offer of "reusable bundles of familiar procedures to improve information security". The core of this approach is to hide the burden of the "traditional risk analysis approach, where the threats are identified first and assigned a probability of occurrence so that suitable security safeguards can be then selected as well as the residual risks can be evaluated". Indeed, IT-Grundschutz's approach is to provide a set of standard security safeguards to counteract typical threats found in a so-called "Information Domain" which can be viewed as a simplified representation of a real situation described in the following five layers:

Layer 1 covers the generic IT security aspects that apply equally to all or most of the IT assets. This applies in particular to generic concepts and the resulting regulations
Layer 2 covers the constructional and physical issues of the infrastructure
Layer 3 covers the security of individual IT systems
Layer 4 covers the security of the network
Layer 5 covers the security of actual applications.

For each layer, IT-Grundschutz Catalogues[92] provide a set of modules that combine, in scenarios, typical threats with their corresponding proven safeguards. These safeguards are listed, grouped by the corresponding lifecycle phase (Planning and design, Procurement, Implementation, Operation, Disposal, and Contingency planning)[93] of the Information Domain for which they should be implemented. IT-Grundschutz Catalogues are the heart of the BSI's methodology; the last English version was published in 2005, and the German version was published in 2007.[94] The document itself contains an introduction, a short description of the methodology, a list of various possible roles found in an Information Domain, and a glossary. Then follow the three main parts: the Module catalogues, the Threats catalogues, and the Safeguard catalogues.

As the IT-Grundschutz is mainly geared towards IT security or information security, all of the risks are analysed against their possible negative impact on the confidentiality, availability and integrity of the information. Impacts are evaluated using a simple qualitative classification: normal, high and very high.

The main description of the methodology itself is to be found in the separate, 93-page document *BSI-Standard 100-2, IT-Grundschutz Methodology*.[95] Its last release, numbered 2.0, was published in 2008. This gives a comprehensive description of the security process that is necessary to achieve an appropriate level of security. The general process consists of the following four groups of steps as shown in Figure 3.1 below. The main risk analysis process consists of the three blocks with the blue background.

---

92 https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html

93 IT-Grundschutz Catalogues, 2005, p. 18.

94 https://www.bsi.bund.de/ContentBSI/grundschutz/grundschutz.html. BSI provides regular updates, in German, for registered users. Registration with the BSI is on a voluntary basis and is free of charge.

95 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile

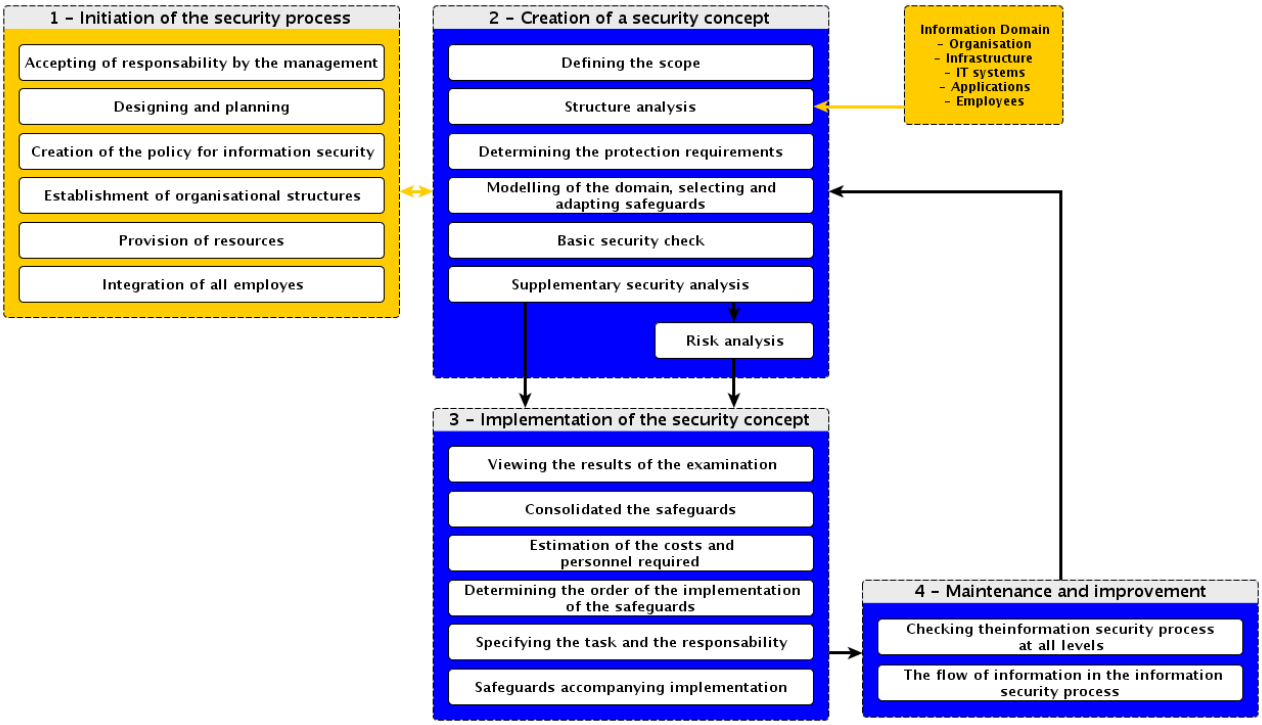


Figure 3.1: Phases of the security process

The risk analysis process is specifically described in a shorter, 23-page document, *BSI-Standard 100-3, Risk analysis based on IT-Grundschutz*.[96] This process is suitable for both existing and planned IT assets. In the first case, the result of the "Modelling" of the Information Domain will be a "Test plan" for carrying out a target or actual comparison while, in the second case, the modelling result will be a "Development concept" with a list of requirements.[97] In case a situation is not described in the IT-Grundschutz Catalogues, the methodology offers room for the determination of additional threats within the risk analysis step.[98]

The BSI has developed a certification scheme for the implementation of IT-Grundschutz, which consists of three levels based on the safeguards implemented. Each safeguard is associated with a category: A for entry level, B for continuation level, and C for certification level, while the additional Z category corresponds to optional measures. Certification at level A requires the measures in A; certification at level B requires the measures in A and B; and certification at level C requires the measures in A, B and C. The certification at level C is compatible with the requirements of ISO/IEC 27001. [99] Finally, as a kind of encyclopedic risk management methodology, IT-Grundschutz tries to cover as many areas and interactions as possible in the Information Domain, and this includes data privacy protection (or Datenschutz in German).

Data privacy protection is an entry in the Module Catalogues with reference B 1.5. However, the module's description is not yet fully integrated into the main document and still appears as

[96] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile
[97] BSI-Standard 100-2 – IT-Grundschutz Methodology, 2008, pp. 61-62.
[98] cf. Determination of additional threats, in BSI-Standard 100-3 – Risk analysis based on IT-Grundschutz, 2008, pp. 12-14.
[99] BSI-Standard 100-2 – IT-Grundschutz Methodology, 2008, pp. 87-88.

separate.[100] This additional module has been designed by "the Federal Data Protection Officer in co-operation with the Technical Working Group of National and State Data Protection Officers. It is oriented towards public bodies at the federal and state levels, private suppliers of telecommunications services and postal services." This 55-page document deals with the relation between data security and data protection, as well as with the roles of the data security officer and the data protection officer. As a German document, it mainly refers to the requirements set out by German laws at the federal and state levels. And obviously, it focuses on the additional threats and safeguards that derive from the requirements of the laws. The following 13 threats are described:

- T 6.1 Missing legal grounds for the processing of personal data
- T 6.2 Violation of the purpose for which the data originally was collected / Violation of the "purpose binding principle"
- T 6.3 Violation of the necessity principle of collecting only personal data when it is needed for the business process
- T 6.4 Absent or poorly implemented data economy or avoidance of data collection during processing of personal data
- T 6.5 Breach of official secrecy during processing of personal data
- T 6.6 Absent or insufficient preliminary checks
- T 6.7 Endangering the rights of the data subject during processing of personal data
- T 6.8 Missing or insufficient safeguards for subcontracted data processing during processing of personal data
- T 6.9 Missing transparency to the data subject and the data protection auditing authorities
- T 6.10 Endangering required control objectives and related security safeguards during processing of personal data
- T 6.11 Missing or insufficient safeguards for the processing of personal data in foreign countries
- T 6.12 Use of illegal automated decision making or reporting procedures during processing of personal data
- T 6.13 Missing or insufficient data protection auditing.

The following 15 corresponding safeguards are also described:

- Planning and design:
    1. S 7.1 (C) Management of data protection
    2. S 7.2 (B) Definition of roles and responsibilities in the area of data protection
    3. S 7.3 (A) Elements of a data protection concept
    4. S 7.4 (A) Determination of the legal framework and preliminary checks for the processing of personal data
    5. S 7.5 (A) Establishment of state-of-the-art of technical and organisational controls when processing personal data.
- Implementation:
    6. S 7.6 (A) Awareness training of personnel involved in the processing of personal data
    7. S 7.7 (A) Organisational procedures to protect the rights of the data subject during the processing of personal data
    8. S 7.8 (A) Registration of procedures and fulfilment of registration requirements

100 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BaustDatenschutz/moduleb01005_pdf.pdf?__blob=publicationFile

for the processing of personal data
9. S 7.9 (C) Data protection approval to operate
10. S 7.10 (A) Registration and regulations for reporting procedures during processing of personal data
11. S 7.11 (A) Regulations for subcontracting during processing of personal data
12. S 7.12 (A) Rules regarding the correlation, linking and usage of personal data during processing.

- Operations:
  13. S 7.13 (A) Documentation of the data protection acceptability of the processing of personal data
  14. S 7.14 (A) Maintenance of data protection during operations
  15. S 7.15 (A) Data processing-compliant disposal and destruction.

Thirteen out of 15 of the above safeguards belong to the A category, which is the first level of requirement for a security policy. If necessary, this demonstrates that data privacy protection is considered as an important topic within a typical security policy.

	Touch point questions	Evidence from IT-Grundschutz
1	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	Yes. The safeguard S 2.340 (A) Observing legal framework conditions makes provision for consideration of any relevant regulation about the information processing whatever is the country. This safeguard belongs to the entry-level category A. Therefore, it is always required. The corresponding threat is T 2.105, Violation of statutory regulations and contractual agreements. Both belong to the module B1.0, IT Security management.
2	Is the RM methodology regarded as a process or is it simply about producing a report?	Yes, it is a continuous process that can be run from the development of any IT system to its completion.
3	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?	As a risk management methodology, it first addresses information security. However, it also has clear provisions for data privacy protection as set out in the module B 1.5, as both can overlap. There is little or no evidence about other types of privacy unless those other types are defined and required by some relevant regulation.
4	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?	It can be used for existing or planned IT systems. In the latter case, it leads to the definition of a development concept. There is no special emphasis on calling for the use of the methodology as early as possible.
5	Does the RM methodology place responsibility for its use at the senior executive level?	It makes provisions for an IT security officer positioned “organisationally as a staff position, meaning a position placed directly on the management level and that does not receive orders from any other position”. Regarding a data protection officer, it says that “the Data Protection Officer must have the right to speak directly and at any time to administration or management, and

	Touch point questions	Evidence from IT-Grundschutz
		must also be informed quickly and in full of any events in the organisation relevant to his or her activities as the Data Protection Officer".
6	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	During the initiation of the security process, it calls for planning and elaborating a strategy as well as for providing the necessary resources to accomplish the tasks. Although it puts an emphasis on the communication and the involvement of the employees, there is little or no evidence about any kind of a consultation strategy with stakeholders.
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	There is little or no evidence about such an environmental scan at the beginning of the process. However, with regard to the "Determination of additional threats", it calls for a search for threats as wide as possible over the Internet.
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	Yes. The Information Domain can range from an entire organisation to a single application, providing that the Information Domain includes whatever is necessary for the target information processing.
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	It makes little or no reference to any stakeholder consultation. However, it makes some provision for using "external knowledge" if appropriate. This external knowledge may reflect the organisation's needs more than the needs of external players.
10	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	Within the flow of information in the information security process, it makes provision for all kind of communication between "superiors", management staff, security team members and employees.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	As an IT and information security management methodology, it is geared towards the identification of risks facing the organisation itself. However, with the provisions made in Module B 1.5 regarding data privacy protection, it also takes into consideration risks to individuals.
12	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	It calls for the use of safeguards whether to achieve risk reduction, avoidance, acceptance or transfer. Any residual risk must be fully documented in order to take an informed decision.
13	Does the RM methodology include provisions for documenting the process?	It includes provisions for full documentation at all stages of the process.

	Touch point questions	Evidence from IT-Grundschutz
14	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?	It says nothing about making documents public.
15	Does the RM methodology call for a review if there are any changes in the project?	As a process running during the entire life cycle of the so-called Information Domain under consideration, it encourages regular reviews of the safeguards as well as regular checks for new threats.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	It mentions internal or external audit as well as a certification scheme by the BSI, which requires an external audit on a regular basis.

Conclusions and recommendations

As a kind of "encyclopedic" information security process, IT-Grundschutz covers in great detail the security side of data protection. Module B 1.5, Data privacy protection, is specifically designed with the requirements of the German federal law for data protection in mind. This module identifies typical threats regarding compliance with the law as well as their corresponding safeguards. Regarding interactions between this methodology and PIA, IT-Grundschutz lacks some components:

- Consultation with stakeholders regarding their perceptions of possible risks arising from the information processing under consideration
- Broader privacy consideration. IT-Grundschutz is not geared towards all types of privacy consideration which could lead risk managers to overlook some threats to individuals
- Environmental scans during the initiation of the security process.

3.2.3 NIST SP 800-39 Managing Information Security Risk

Managing Information Security Risk (SP 800-39, 2011), published by the US National Institute of Standards and Technology (NIST), is congruent with, and complementary to, NIST 800-30 (2012) and guidance on other areas of organisational risk management as part of an Enterprise Risk Management (ERM) programme. ISO 31000 is cited. Although the writing is wholly new (albeit with some repetition of diagrams), there are considerable overlaps with 800-30, although the latter focuses more on risk assessment and 800-39 is more holistic and emphasises other aspects of risk management. Neither of these NIST publications embraces privacy or data protection as an important element, and almost completely ignore it. Because of this close relationship between the two documents, many details of 800-30 that area described elsewhere in this report will not be repeated here. However, 800-39 develops or emphasises certain elements, explains certain items at greater length, or introduces a number of new and partly different ones. The following are probably the most important different emphases:

- governance and governance models

- the "risk executive (function)"
- risk tolerance and uncertainty
- enterprise and information security architectures
- trust and trust models
- organisational culture
- the relationship among key concepts
- risk responding and monitoring following assessment
- roles and responsibilities.

The main purpose, as in 800-30, is *information security*. Many types of organisational risk are identified: "program management risk, investment risk, budgetary risk, legal liability risk, safety risk, inventory risk, supply chain risk, and security risk". Privacy risk is absent. "Risk" is defined for present purposes as "information security risk from the operation and use of organizational information systems including the processes, procedures, and structures within organizations that influence or affect the design, development, implementation, and ongoing operation of those systems." The document emphasises that this must be a matter for senior executives and leaders, and not confined to a technical "stovepipe" in the organisation, separate from general management. Senior personnel are therefore given risk management responsibilities and are to be accountable for their risk management decisions.

There is also an emphasis on "tools, techniques, and methodologies" to be identified for assessing, developing courses of action, and determining the sufficiency, correctness and effectiveness of risk responses. As in 800-30, 800-39 analyses the processes and activities at the three organisational tiers, and adopts the fourfold frame-assess-respond-monitor risk-management process concept. A new concept is that of *risk executive (function)*. This is established at the top (organisational) tier as a crucial part of the governance and decision-making structure for risk management; it "serves as the common risk management resource for senior leaders/executives, mission/business owners, chief information officers, chief information security officers, information system owners, common control providers, enterprise architects, information security architects, information systems/security engineers, information system security managers/officers, and any other stakeholders having a vested interest in the mission/business success of organizations."

Risk tolerance is an important element of *risk framing*, and indicates "the level of risk or degree of uncertainty that is acceptable to organizations", constraining risk management decisions and shaping oversight, the rigour of the risk assessment, and the responsive strategies adopted. The document explains *enterprise and information security architectures* at length in its discussion of Tier 2 (mission/business process). These architectures have much to do with the organisation's resilience to threats. In particular, the information security architecture "incorporates security requirements from legislation, directives, policies, regulations, standards, and guidance". The description of enterprise architecture includes "privacy" as one of the risk-reduction aims for the full, organisation-wide integration of management processes, but this is not explained.

The concepts of *trust* and *trustworthiness* are deemed important factors in risk decision-making, with "trust" defined as "a belief that an entity will behave in a predictable manner in specified circumstances. The entity may be a person, process, object or any combination of such components." An Appendix sets out a number of trust models as alternative ways for organisations to obtain levels of trust needed to form partnerships and collaborations and to share information. Trustworthiness relates to assurance about IT products and systems in the

face of threats, and susceptibility to attack shapes the acceptability of levels of risk. *Organisational culture* (values, beliefs and norms influencing behaviour and action) is a dimension that 800-39 treats at length, as it affects many if not all the other elements of risk management. Where the cultures of two organisations differ, or where parts of the same organisation have different cultures, these "disconnects" may be palpable in terms of information-sharing: "An example of an internal disconnect can be observed in a hospital that emphasizes different cultures between protecting the personal privacy of patients and the availability of medical information to medical professionals for treatment purposes." We may note that this is an almost isolated mention of "privacy" in 800-39, and that the example is a classic data protection issue that PIA would encounter in its analysis of an organisation's processes. But 800-39 offers no guide to the resolution of such clashes of culture and the information-sharing decisions that are implicated. A section on the relationship among all the key risk concepts (governance, risk, tolerance, trust, culture and investment strategy) then follows, showing their inter-relationship and the importance of the risk executive (function)'s cognisance of this.

NIST 800-39 moves on to discuss the process for managing risk through the familiar stages of framing, assessing, responding and monitoring, describing each with more fine-grained sub-processes. This analysis goes beyond 800-30's focus on risk assessment to describe more fully the stages of *responding to risk* and *risk monitoring*, including several steps in each. There is a large Appendix that delineates the *roles and responsibilities* of key organisational participants. Although they are not here referred to as "stakeholders", many if not all of them are elsewhere so described. These roles include: CEO, risk executive (function) – an individual or a group, CIO, information owner/steward, senior information security officer, authorising official, authorising official designated representative, common control provider, information system owner, information system security officer, information security architect, information system security engineer, and security control assessor. If, through an "open door", a PIA were to be grafted into the risk management process covered by 800-39, these personnel and their differing but overlapping responsibilities, and perhaps their differing cultures (and what those cultures might indicate with regard to information processes that bear upon privacy) would have to be factored into the PIA routine.

	Touch point questions	Evidence from NIST 800-39
1	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	It mentions legislation but also includes "directives, policies, regulations, standards, and guidance".
2	Is the RM methodology regarded as a process or is it simply about producing a report?	It is a process.
3	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?	NIST 800-39 barely mentions privacy and the example it mentions is of information privacy. Broadening could perhaps be done within the scope of the RM, but adopting a conception of privacy that went beyond information *security* would be a prerequisite for the organisation.
4	Does the RM methodology say that it should be undertaken when it is still	The RM exists at all stages of a project and continuously.

	Touch point questions	Evidence from NIST 800-39
	possible to influence the development of the project?	
5	Does the RM methodology place responsibility for its use at the senior executive level?	The RM involves responsibilities (activities) at several levels. Top-tier responsibility is heavily discussed but responsibilities are also set forth in many other places and among many other roles.
6	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	Not so explicitly for this RM, but holistically. There is a *security* plan. There is also internal consultation between senior executives and the "risk executive (function)" about the risk-assessment process (e.g., framing, etc.).
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	The *Guide* mentions many other NIST risk, security and other publications, as well as ISO and other standards.
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	This scale does not seem to apply to RM, except perhaps in terms of *risk aggregation*, which is only mentioned in 800-39 but more fully discussed in 800-30.
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	There are frequent mentions of "stakeholders", and the *roles* that are delineated describe who they are and what their responsibilities are. Their perspectives are implicitly recognised. Presumably they would be a PIA's "stakeholders" as well, but there are also external ones (other organisations).
10	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	Communication is not separately and explicitly discussed, but is mentioned and is implicit in RM processes, especially regarding role-coordination.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	This RM is almost exclusively non-individual in focus.
12	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	Alternative actions to mitigate risk are discussed as part of risk response, but not concerning any privacy impact.
13	Does the RM methodology include provisions for documenting the process?	Documentation is mentioned in a number of places, particularly in describing the role of the "common control provider".

	Touch point questions	Evidence from NIST 800-39
14	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?	Nothing is mentioned about publication.
15	Does the RM methodology call for a review if there are any changes in the project?	Continuous monitoring is important to RM.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	Review of risk management decisions is part of *maintaining* the RM.

Conclusions and recommendations

This is an elaborate document that, read together with NIST SP 800-30, gives a highly detailed and elaborate descriptive guide to risk management in all its stages, procedures, structures and thought-processes. As with 800-30, but perhaps to a lesser extent, there may be "touch points", "open doors", and other affordances in NIST 800-39 and in the PIA Handbook that could be worth developing. Although hardly any mention is made of privacy, the specific focus of 800-39 on security risk should not rule this out, especially if 800-30 is implemented in conjunction with it and if the latter can be oriented more firmly towards PIA. If PIA can be inserted into the security concerns of 800-39, PIA responsibility could be grafted onto the role of "risk executive (function)" in the governance and decision-making structure for risk management. The emphasis on organisational culture, and the example of cultural "disconnect" between attitudes towards data-sharing, could be a doorway for helping organisations resolve such dilemmas through the analysis that PIA would bring to these situations. In addition, the "stakeholder" framework could be adapted to PIA purposes.

3.2.4 ISACA and COBIT

ISACA (originally known as Information Systems Audit and Control Association) originated in 1969 as the EDP Auditors Association. Since those origins, the members of ISACA, who serve in a variety of IT-related positions, are found in 190 chapters in over 180 countries, and currently exceed 100,000 in number. ISACA established a research affiliate, the IT Governance Institute (ITGI), in 1998. The focus of the organisation is upon developing knowledge around information systems assurance, control, and security, as well as governance of IT and related risk and compliance issues. ISACA developed and administers several certifications, including the Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), and Certified in the Governance of Enterprise IT (CGEIT).[101]

COBIT (Control Objectives for Information and related Technology), originally published in 1996 and now released in version 5, is a process framework for IT and encompasses

[101] www.isaca.org

frameworks for value of IT business investments (Val IT) and for risk management (Risk IT). COBIT, like other IT governance frameworks, focuses upon the efficient and effective use of IT assets, and includes the following key areas: strategic alignment, value delivery, risk management, resource management, performance management. [102]

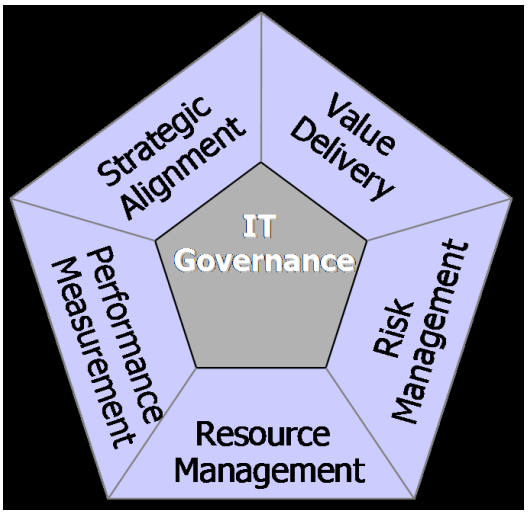


Figure 3.2: IT Governance Model

COBIT itself is a framework and does not aim to provide in-depth guidance on every aspect of managing and governing IT. COBIT refers users of the framework to other more detailed standards such as ITIL (for service delivery), CMM (for solution delivery), ISO 17799 (for information security) and PMBOK or PRINCE2 (for project management). Over time, more than 40 international IT standards, frameworks, guidelines, etc. have been consulted for the development of COBIT, including notably those published by COSO, OGC, ISO, SEI, PMI, and ISF. The COBIT framework ties together business requirements with IT processes and IT resources:

Business requirements	**IT processes**	**IT resources**
Effectiveness Efficiency Confidentiality Integrity Availability Compliance Reliability	Domains Processes Activities	Applications Information Infrastructure People

The process model for COBIT comprises four domains with 34 generic processes aimed at "managing the IT resources to deliver information to the business according to business and governance requirements". The four domains are 1) plan and organise, 2) acquire and implement, 3) deliver and support, and 4) monitor and evaluate. The COBIT framework provides a process description, control objectives, management guidelines and a maturity model for each distinct process within these domains.

The process description indicates which IT process is controlled, how it satisfies business requirements, and how it is achieved and measured. The process is decomposed into a series

[102] Bentley, William, and Peter T. Davis, *Lean Six Sigma Secrets for the CIO*, CRC Press, 2010.

of specific activities. The management guidelines define which processes provide inputs, and which outputs are created by the process. A RACI (Responsible, Accountable, Consulted, or Informed) chart is provided for each activity in the process and goals and metrics for the process are established.

Within the "plan and organise" domain, 10 processes are described. They concern defining a strategic IT plan; defining the information architecture; determining the technological direction; defining the IT processes; organisation and relationships; managing the IT investment; communicating management aims and direction; managing IT human resources; managing quality; assessing and managing IT risks; and managing projects. Key areas where privacy and data protection elements may be introduced are within the following activities:

PO2.3 - Data Classification Scheme
PO2.4 - Integrity Management
PO4.8 - Responsibility for Risk, Security and Compliance
PO6.2 - Enterprise IT Risk and Control Framework
All activities associated with PO9 Assess and Manage IT Risks
PO10.4 - Stakeholder Commitment

The domain of "acquire and implement" includes seven processes: they include identifying automated solutions; acquiring and maintaining application software; acquiring and maintaining technology infrastructure; enabling operation and use; procuring IT resources; managing changes; and installing and accrediting solutions and changes. Key areas where privacy and data protection elements may be introduced are within the following activities:

AI1.2 - Risk Analysis Report
AI2.1 - High-level Design
AI2.2 - Detailed Design
AI2.3 - Application Control and Auditability
AI3.2 - Infrastructure Resource Protection and Availability
AI6.2 - Impact Assessment, Prioritisation and Authorisation

The "deliver and support" domain comprises 13 processes. These processes include defining and managing service levels; managing third-party services; managing performance and capacity; ensuring continuous service; ensuring systems security; identifying and allocating costs; educating and training users; managing service desk and incidents; managing the configuration; managing problems; managing data; managing the physical environment; and managing operations. Key areas where privacy and data protection elements may be introduced are within the following activities:

DS2.3 - Supplier Risk Management
All activities associated with process DS5 - Ensure Systems Security
DS11.1 - Business Requirements for Data Management
DS11.2 - Storage and Retention Arrangements
DS11.6 - Security Requirements for Data Management

The fourth domain, "monitor and evaluate", comprises four processes that include monitoring and evaluating IT performance; monitoring and evaluating internal control; ensuring compliance with external requirements; and providing IT governance. Key areas where privacy and data protection elements may be introduced are within the following activities:

ME3.1 - Identification of External Legal, Regulatory and Contractual Compliance Requirements
ME3.2 - Optimisation of Response to External Requirements
ME3.3 - Evaluation of Compliance with External Requirements
ME3.4 - Positive Assurance of Compliance
ME3.5 - Integrated Reporting

The COBIT framework has developed over the past decade and a half, with the most recent update to COBIT published in 2012 as COBIT 5. COBIT 5 now encompasses the additional Risk IT and Val IT frameworks, whose relationship to COBIT are shown in Figure 3.3 below.

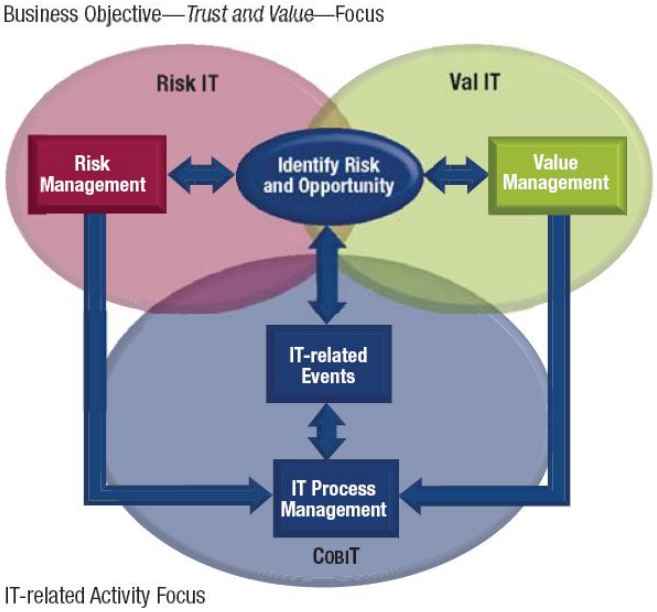


Figure 3.3: COBIT and related frameworks

Of particular interest in this context is Risk IT, which was originally published in 2009, based upon the then current version of COBIT (4.1). "The Risk IT framework is based on the principles of enterprise risk management (ERM) standards/frameworks such as COSO ERM and AS/NZS 4360 (soon to be complemented or replaced by ISO 31000) and provides insight on how to apply this guidance to IT." The process model presented under Risk IT includes three domains: risk governance, risk evaluation, and risk response. In turn, each of these domains includes three defined processes

Risk governance	Risk evaluation	Risk response
RG1 Establish and maintain a common risk view RG2 Integrate with ERM RG3 Make risk-aware business decisions	RE1 Collect data RE2 Analyse risk RE3 Maintain risk profile	RR1 Articulate risk RR2 Manage risk RR3 React to events

The following examines COBIT and Risk IT within the context of how they relate to the key touch points for PIA, and how and where PIA may fit into the framework as it currently exists.

	Touch point questions	Evidence from COBIT
1	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	In COBIT, Process ME3.3 – Evaluation of Compliance with External Requirement provides for this type of review.
2	Is the RM methodology regarded as a process or is it simply about producing a report?	It is a framework that supports the application of other risk management methodologies, and provides in that context a strategic approach to risk, which is cyclical in nature.
3	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?	It is expansive and addresses a broad range of risks that may be applicable. Privacy is not specifically identified, but is included within the approaches taken for ensuring compliance.
4	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?	It is aimed at tying business value to IT processes, including those related to risk management. As such, risks are contemplated in the earliest stages of a project or programme and continually evaluated and responded to.
5	Does the RM methodology place responsibility for its use at the senior executive level?	Yes. IT risk management defined within the COBIT and Risk IT frameworks is driven by a governance model that relies upon a definition of risk appetite/tolerance at strategic levels in the organisation (i.e., Board or most senior level), and integrates with enterprise-level risk management.
6	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	COBIT calls for strategic planning in the Plan and Organize domain, and Risk IT establishes activities to be pursued in the Risk Governance domain, each involving a broad range of stakeholders.
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	While there is no explicit call for an environmental scan, one of the four domains, “Monitor and Evaluate”, primarily focuses upon external regulatory and compliance issues, and should typically lead to such a generalised environmental scan.
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	No.

	Touch point questions	Evidence from COBIT
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	Within the "Plan and Organize" domain, the activity PO10.4 is aimed at ensuring all stakeholders are engaged and provide inputs to the definition and execution of the project.
10	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	Process PO6 (within the "Plan and Organize" domain), Communicate Management Aims and Direction, includes the activity PO6.5, Communication of IT Objectives and Direction. This activity ensures that all stakeholders are provided with an awareness and understanding of business and IT objectives and direction.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	It defines the processes related to the identification of risk within the PO9 "Assess and Manage IT Risks" process and its related activities. In addition, these processes are defined in more detail in the related Risk IT framework.
12	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	It calls for high-level and detail design (AI2.1 and AI2.2) to be completed within the context of the organisation's technological direction and information architecture, which standards should be defined to avoid negative impacts.
13	Does the RM methodology include provisions for documenting the process?	Numerous artefacts are expected to be produced within the framework, enabling communication of outputs from one process as inputs to other processes, creating effective linkages of the business and IT processes within the various domains.
14	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?	No. There is no discussion of communication outside of the defined stakeholders.
15	Does the RM methodology call for a review if there are any changes in the project?	Risk management is viewed as a continuous cycle and is applied to both projects and ongoing IT services.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	In the "Monitor and Evaluate" domain, the activity ME3.4, Positive Assurance of Compliance, is aimed at ensuring that "any corrective actions to address any compliance gaps have been taken by the responsible process owner in a timely manner."

Conclusions and recommendations

For the purpose of identifying a window for inclusion of PIAs within the COBIT framework, our assessment leads us to believe that many of the key elements of PIA are implicitly included in the framework, especially with respect to the processes in the "Monitor and Evaluate" domain, which calls for adherence with external compliance and regulatory factors. Moreover, as a framework, where COBIT relies upon other standards such as ITIL, ISO 31000, COSO, and others, inclusion of PIA within those other standards will necessarily roll-up into the processes observed by COBIT user organisations. As an alternative approach, it may be valuable to develop a white paper or case study identifying linkages between PIA and COBIT, working with ISACA to introduce them into their certification programmes or simply for dissemination within their global membership.

3.3 RISK ANALYSIS METHODOLOGIES

3.3.1 CRAMM

CRAMM was originally developed by the CCTA (Central Computer and Telecommunications Agency) of the UK government as the CCTA Risk Analysis and Management Method (CRAMM) in 1985. Its original purpose was to provide government departments with a method that would be specifically aimed at performing security reviews for information systems. Since that time the methodology has been developed, both from the perspective of content and of technological support. The method was commercialised as a tool by a UK firm (Insight Consulting)[103] and subsequently by Siemens, who now publishes the tool under version 5.1.[104]

The ongoing use of CRAMM, in the UK or elsewhere, appears to be significantly diminished over the time since its original development for use by government agencies. This observation is based upon the scarcity of reference materials or media references, as well as upon responses to the surveys conducted in conjunction with (and preceding) this study. According to adoption rate details from the current CRAMM toolkit publisher, Siemens, there are over 600 copies of the software in use in 23 countries. PRINCE2, which is now used by most UK government agencies as a project management standard, includes the M_o_R as the standard for risk management, and offers a government-sanctioned alternative to CRAMM for risk management. The current version of CRAMM includes support for certifications against BS7799 (as well as the related ISO 27000 series of standards). The CRAMM countermeasures reflect the BS7799: 2005/ISO 27001 controls.

The CRAMM method is broken down into three stages or phases:

- identification and valuation of assets – of the 400 types of assets supported, they broadly encompass data, physical assets and systems;
- assessment of threats and vulnerabilities – the tool supporting the CRAMM method includes 38 types of threats and 25 different types of impact;
- analysing risk and managing risk, including identification and prioritisation of countermeasures – the countermeasure library for the 5.1 version of the CRAMM toolkit includes over 3,500 generic controls, and seven different measures of risk.

[103] SANS Institute, "A Qualitative Risk Analysis and Management Tool - CRAMM", 2002.
[104] Siemens Enterprise, "CRAMM v5.1 Information Security Toolkit".
http://www.cramm.com/downloads/datasheets.htm

The following table examines CRAMM within the context of how it relates to the key touch points for PIA, and how and where PIA may fit into the framework as it currently exists. Due to the limited availability of information about CRAMM in the public domain, the analysis that can be completed here is quite limited.

	Touch point questions	Evidence from CRAMM
1	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	It includes support for BS7799: 2005 and ISO 27001.
2	Is the RM methodology regarded as a process or is it simply about producing a report?	CRAMM focuses on performing a complete risk assessment for information security, and includes both a toolkit to support the process and reporting elements to communicate the results of that assessment.
3	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?	It focuses on threats, vulnerabilities and the risks they represent, not particularly upon privacy (except where privacy is identified as a risk to the assets).
4	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?	The risk assessment is intended to be performed on a cyclical, ongoing basis, as a matter of information security.
5	Does the RM methodology place responsibility for its use at the senior executive level?	No. There is no focus on senior executives in any accessible literature. However, a published review of the CRAMM toolkit points out that it has the ability to present results to management using graphs and reports produced by the tool.[105]
6	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	No. There is no evidence to support this.
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	No. There is no evidence to support this. Published reviews of CRAMM do mention that the data entered into the toolkit can be captured and re-used when a subsequent risk assessment is performed, providing a basis for comparison.[106]

[105] Kaner, Ece, "Integrated Approach to Information Risk Assessment", Concordia University, Montreal, June 2008.
[106] Ibid.

	Touch point questions	Evidence from CRAMM
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	The method is driven by assessing risk around the various assets of the organisation, not on a project basis. Thus, there is no public evidence to support that this is the case.
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	Accessible information is insufficient to determine whether this is the case.
10	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	Accessible information is insufficient to determine whether this is the case.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	The focus of threat, vulnerability and risk assessment is based upon the assets of the organisation. This includes up to 400 different types of assets, including data.
12	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	Countermeasures are selected as responses to the identified risks. As part of that evaluation, CRAMM includes the assignment of costs associated with mitigating risks, which may be inferred to provide for a business justification, though it is not necessarily a complete view of the business need.
13	Does the RM methodology include provisions for documenting the process?	The CRAMM toolkit creates graphs, charts and reports to document the results of the risk assessment.
14	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?	No. There is no evidence to support this.
15	Does the RM methodology call for a review if there are any changes in the project?	CRAMM calls for a cyclical re-assessment of risk on an ongoing basis.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	It provides the ability to store the results of one assessment and compare it to the next assessment, which would give the assessor a view as to whether risk-related recommendations have been implemented; however, the frequency of the risk assessment is at the core of whether this is an effective tool for compliance with such recommendations.

Conclusions and recommendations

Based upon our survey of UK organisations and a desktop review of the marketplace, the CRAMM method has limited application and use at this time, and appears to have been largely supplanted by other methods. Moreover, given that CRAMM provides support for ISO 27001 and BS7799, it would seem to be a more effective approach to address any modifications required to risk assessment within those contexts (as well as within the risk management elements of PRINCE2) to enable the uptake of PIA within organisations.

3.3.2 EBIOS

EBIOS stands in French for "Expression des Besoins et Identifications des Objectifs de Sécurité", which in English means "Expression of Needs and Identification of Security Objectives".[107] This risk management method was created in 1995 by the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI),[108] the French Network and Information Security Agency (FNISA), and was first released in 1997.[109] Since then, there have been two major updates: in 2004 and in 2010. Among other improvements, the revisions have introduced better compatibility with international standards on information security management and risk management, namely ISO 27001, ISO 27005, ISO Guide 73 and ISO 31000.

To date, the EBIOS method is only available in French; however, an English version is awaiting approval and should be available soon. As such, EBIOS is mainly used in France, where it is recommended for public administrations and for private companies that are carrying out contracts for the Defence Ministry or that have strong needs in terms of information security. EBIOS is also used abroad in French-speaking countries, and ENISA has drawn on EBIOS. The use of EBIOS is suitable for various types of structure, ranging from small and medium-sized companies and local authorities to multi-national companies as well as international organisations. Since 2006, EBIOS has been supported by the "Club EBIOS",[110] which is a user group, independent of ANSSI, formed by public and private sectors organisations as well as individual experts.

EBIOS is a high-level method for risk management. It is mainly an information security method; however, due to its modular and flexible approach to risk management, it is general and powerful enough to be used in other sectors as well.[111] It is a kind of tool-box which comes as a set of two main documents. The 97-page Risk Management Method[112] gives an overview of risk management and then focuses on information security (Chapter 1). It explains what EBIOS is and how it works (Chapter 2), and describes each of the activities that make up the approach (Chapter 3). A demonstration of the coverage of international standards (Appendix A), and a glossary and some useful references (Appendix B) supplement the

[107] http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html
[108] http://www.ssi.gouv.fr/
[109] EBIOS V1
[110] http://www.club-ebios.org
[111] Health and safety, environment protection, management of legal risks, etc.
[112] *EBIOS 2010 – Méthode de gestion des risques*, ANSSI. http://www.ssi.gouv.fr/IMG/pdf/EBIOS-1-GuideMethodologique-2010-01-25.pdf

document. The 51-page "Knowledge base"[113] is a catalogue describing the types of supported assets (Chapter 1); the types of impact (Chapter 2); the types of threat source (Chapter 3); generic threats and vulnerabilities (Chapter 4); and generic controls (Chapter 5). Both documents are supplemented by free software[114] and by "@RCHIMED: A case study",[115] which is a full 69-page example detailing the use of EBIOS.

Within EBIOS, an information security risk is a combination of the following four elements:

- a threat source,
- a threat,
- a vulnerability,
- an impact.

Thus, EBIOS focuses on the identification of those four elements as well as on the proposal of various scenarios that combine them in likely ways. Through this, EBIOS allows the risk manager to assess and treat risks. It also provides all the necessary elements for communication within the organisation and its partners as well as the validation of risk treatment.

EBIOS is an iterative method suitable for producing many types of deliverables ranging from an organisation's information security policy and a security strategy to a risk map or a treatment plan. Since its last release in 2010, EBIOS has been restructured into five modules to comply with the requirements of ISO 27001, ISO 27005 and ISO 31000. Figure 3.4 below shows the organisation of those modules as a five-step process.

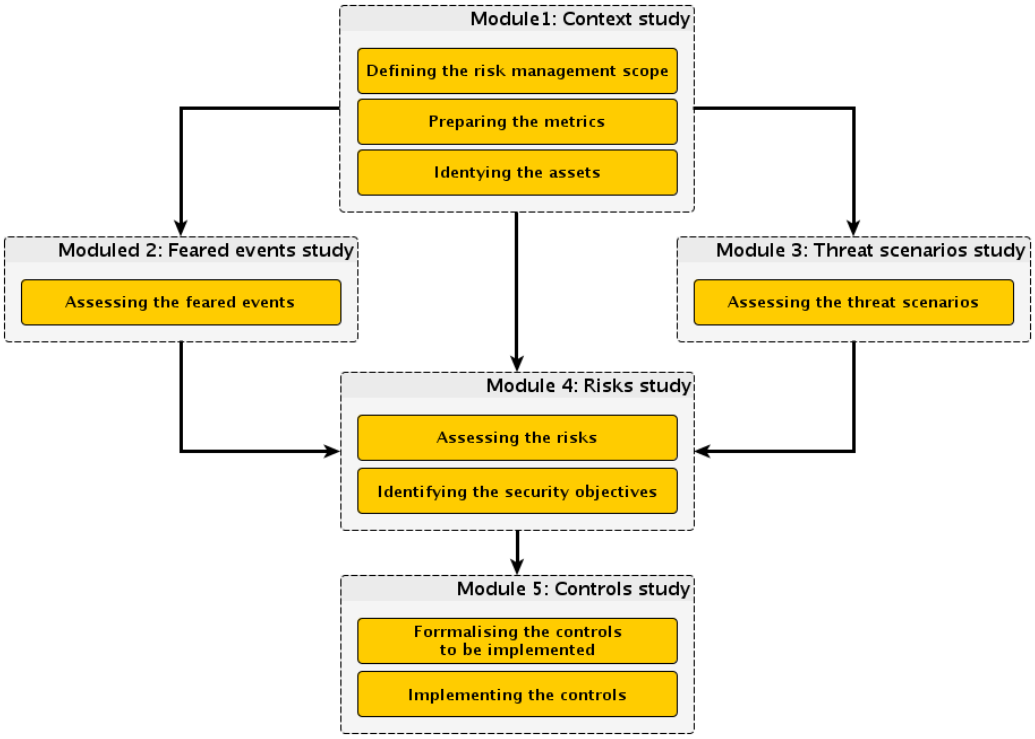


Figure 3.4: EBIOS's five-step process

[113] *EBIOS 2010 – Base de connaissances*, ANSSI. http://www.ssi.gouv.fr/IMG/pdf/EBIOS-2-BasesDeConnaissances-2010-01-25.pdf
[114] https://adullact.net/projects/ebios2010/
[115] http://www.ssi.gouv.fr/IMG/pdf/EBIOS-EtudeDeCas-Archimed-2010-01-25.pdf

Module 1 establishes the context, the scope of the risk management, the metrics and boundaries of the study. It also identifies the primary assets, the supporting assets on which they depend, and the parameters to be taken into account in the risk treatment. Module 2 contributes to risk assessment. It helps identify and estimate the security needs of the primary assets (in terms of availability, integrity, confidentiality, etc.), all the possible impacts (on the missions, the safety of people, financial, legal, image, environment, third parties and others, etc.) in the event of non-compliance with these needs, and the threat sources (human, environmental, internal, external, accidental, deliberate, etc.) that then contribute to the formulation of the feared events. Module 3 is also part of the risk assessment. It involves identifying and assessing the scenarios that can generate the feared events and thus be part of risks. The risk manager must carefully study the threats generated by the source of threats as well as all of the exploitable vulnerabilities. Module 4 highlights the risks for the organisation by checking the feared events against the threat scenarios. It also describes how to estimate and evaluate these risks and how to identify the security objectives that need to be achieved to treat them. Finally, Module 5 focuses on risk treatment. It explains how to specify the controls to be implemented, how to plan the implementation of these controls and how to validate the risk treatment and residual risks.

Possible "touch points" between the PIA Handbook and EBIOS are shown below:

	Touch points questions	**Evidence from EBIOS**
1	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	Yes. Within Module 1, Action 1.1.4, "Identify the parameters to be taken into account", makes specific provisions for taking into account any laws, rules and regulations that may have an effect on risk management. Within Chapter 5, "Generic controls" of "EBIOS 2010 – Base de connaissances", provisions are made for general compliance, and item 15.1.1, "Identification of the legislation in force", makes specific provisions for identifying "all of the legal, regulatory and contractual requirements in force for each information system and for the organization."
2	Is the RM methodology regarded as a process or is it simply about producing a report?	Yes. It is a fully iterative process which should be used in each phase of a project's life cycle.
3	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?	It is mainly geared towards information security. As such, it mainly focuses on information protection in terms of availability, confidentiality and integrity. It can be used for the protection of any kind of information, including information privacy. This is set out in Module 1, Action 1.3.1, "Identify the primary assets, their relations and their trustees", which makes specific provisions for personal data as set out in the French law for personal data protection. Item

	Touch points questions	Evidence from EBIOS
		15.1.4, "Data protection and confidentiality of information relating to private life", also makes specific provisions for that. There is little or no evidence about other types of privacy, although it does refer to human impacts; however, as a generic risk management methodology, other types of privacy could easily be included in the scope of a study.[116]
4	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?	Yes. It is suitable for any type of system either in the development phase or in production. It clearly makes provision for starting as soon as a new service or system comes into consideration in order to be able to influence the design and to make the necessary choices before investing too much to be able to reverse the decision.
5	Does the RM methodology place responsibility for its use at the senior executive level?	There is no clear provision for that. However, as a risk management methodology suitable for a whole organisation as well as for producing high-level documents, such as security policies, one can assume that use of EBIOS must have some engagement with senior management.
6	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	Yes. Within Module 1, Action 1.1.1, "Scope the risks study", makes provision for formalising the aims of the study in terms of intention and deliverables as well as how it is to be conducted. In addition, EBIOS includes provisions for identifying all relevant stakeholders to be involved, and for consulting on the risks.
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	Yes. Within Module 1, Action 1.1.2, "Describe the general context", includes a study of the general context (external and internal). This includes the environment: social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive, and at international, national, regional and local levels; the factors and trends that have a determining impact on the objectives, as well as the relations with external stakeholders, their perceptions and their values.

[116] In fact, this has been done by the French Data Protection Authority (CNIL) with its two guides, "Methodology for privacy risk management" and "Measures for the privacy risk treatment". Both were published in 2012 and are part of this study.

	Touch points questions	Evidence from EBIOS
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	Yes. It can easily scale to be used on a whole sector of activity, part of an organisation, an information system, an IT system, a network of systems, an application, or even a single component of a product.
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	Yes. It makes clear provisions for "Communication and consultation on the risks" and says that involvement of all relevant stakeholders is necessary for the appropriate definition of the context and for taking their interests into consideration. Within Module 1, Action 1.1.3, "Delimit the boundaries of the study", also makes specific provision to identify and clearly define the participants of the study.
10	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	Yes. It makes specific provision for including communication in each activity within its process. Communication is also considered as a key activity within the risk management process.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	Yes. Risk analysis is done within Module 4, Action 4.1.1, "Analyse the risks", which is based on the results of Action 2.1.1, "Analyse all of the feared events" within Module 2, and Action 3.1.1, "Analyse all of the threat scenarios" within Module 3.
12	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	Yes. This is done along with Module 5, "Study of the controls", which aims to determine the methods and means to treat the risks. Action 5.1.2 as well as Action 5.2.2, "Analyse the residual risks", make specific provisions for analysing the residual risks before the implementation of the controls, for the former, and after the implementation of the controls, for the latter.
13	Does the RM methodology include provisions for documenting the process?	Yes. All decisions must be fully documented. Furthermore, various documents may be an output at any step in the process. These range from general information security policy to rational expression of security objectives statements.[117]
14	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?	No. There is little or no evidence about public release of any document resulting from the process.

[117] Ibid., p. 13

	Touch points questions	Evidence from EBIOS
15	Does the RM methodology call for a review if there are any changes in the project?	Yes. Within EBIOS, a "Risk monitoring and review" task is included in all module activities.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	It does not include explicit provisions for audits. However, within Module 5, Action 5.2.3, "Grant security accreditation", which consists of organising the formal validation of the study's conclusions, implies a decision based on the results of an audit, either internal or external.

Conclusions and recommendations

EBIOS is a high-level risk management methodology designed for information security, but is flexible and powerful enough to be suitable for any kind of risk analysis. EBIOS includes many provisions that make it suitable for PIAs. In fact, the Club EBIOS has published two examples of its use for privacy protection.[118] However, to be usable right out of the box for privacy protection, EBIOS has yet to be adapted with the privacy requirements set out by laws and regulations. Fortunately this work has been done in 2012 by the French Data Protection Authority (CNIL), which has published two guides in this regard.[119]

3.3.3 OCTAVE®

OCTAVE®[120] stands for "Operationally Critical Threat, Asset and Vulnerability Evaluation". It is a "framework" for security evaluation that was first published by the Software Engineering Institute (SEI) at Carnegie Mellon University (CMU) in 1999. It was developed in the USA to help the US Department of Defense (DoD) to address the requirements set out by the Health Insurance Portability and Accountability Act (HIPAA)[121] for personal health data protection.

The heart of OCTAVE is a set of criteria that are described in "OCTAVE^{SM} Criteria, Version 2.0"[122], a report of 143 pages, published in 2001. Those criteria form the basis from which various methods have been and can be derived.

To date, three methods consistent with OCTAVE criteria have been published by SEI:

- OCTAVE Method is the original one, published in 2001. The method is described in

[118] Grall, Matthieu, *Études de cas: Médecine du travail*, Club EBIOS, 2011. http://www.club-ebios.org/site/documents/ClubEBIOS-EtudeDeCas-MedecineTravail-2011-11-29.pdf. Grall, Matthieu, Études de cas: Géolocalisation de véhicules d'entreprise, Club EBIOS, 2012. http://www.club-ebios.org/site/documents/ClubEBIOS-EtudeDeCas-Geolocalisation-2012-12-15.pdf

[119] "Methodology for privacy risk management" and "Measures for the privacy risk treatment" both are included in this study

[120] OCTAVE is registered in the U. S. Patent and Trademark Office by Carnegie Mellon University.

[121] US Department of Health & Human Services, The security rules. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/

[122] Alberts, Christopher J., and Audrey J. Dorofee, *OCTAVE^{SM} Criteria, Version 2.0*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2001. https://www.cert.org/archive/pdf/01tr016.pdf

OCTAVE[sm] *Method Implementation Guide*,[123] a set of 18 volumes describing the entire process, step by step. The OCTAVE method has been designed for large, multi-layered, hierarchical organisations with more than 300 employees that maintain their own IT infrastructures.

- OCTAVE-S is the OCTAVE method streamlined for small companies with fewer than 100 employees, a flat hierarchy, and that are mostly outsourcing their IT infrastructure. It takes into account the limited means and unique constraints usually found in small organisations. The first version of OCTAVE-S was published with the version number 0.9 in 2003, while the last version was published in 2005. The method is described in *OCTAVE*®*-S Implementation Guide*,[124] which is a set of 10 volumes.
- OCTAVE Allegro is the last member of the OCTAVE family, published in 2007. It is described in the 116-page *The OCTAVE Allegro Guidebook*[125]. OCTAVE Allegro is a streamlined version of the previous methods. It is an information-centric risk assessment method which specifically focuses on information assets "in the context of how they are used, where they are stored, transported, and processed, and how they are exposed to threats, vulnerabilities, and disruptions as a result".[126] As such, this variant of the OCTAVE method does not consider all of the possible types of assets but rather focuses on assets directly related to information, the so-called "information containers".

Although the three OCTAVE-based methods differ slightly in their processes and steps, they all rely upon the same OCTAVE criteria that form their common foundation. OCTAVE criteria consist of a set of 10 high-level principles that "are the fundamental concepts driving the nature of the evaluation", and from which a set of 15 attributes are derived. "Attributes are the distinctive qualities, or characteristics, of the evaluation. They are the requirements that define the basic elements of the OCTAVE approach and define what is necessary to make the evaluation a success from both the process and organizational perspectives."[127]

Principles and attributes are mapped together in the Table 3.1 below.

Mapping of principles to attributes	
Principles	**Attributes**
Information security risk evaluation principles	
Self-direction	• RA 1 Analysis team • RA 2 Augmenting analysis team skills
Adaptable measures	• RA 3 Catalog of practices

[123] Alberts, Christopher J., and Audrey J. Dorofee, *OCTAVE*[sm] *Method Implementation Guide Version 2.0*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2001. https://www.cert.org/octave/octavemethod.html (under the download link which requires a registration)

[124] Alberts, Christopher, Audrey Dorofee, James Stevens and Carol Woody, *OCTAVE*® *Implementation Guide Version 1.0*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2001. https://www.cert.org/octave/octaves.html (under the download link which requires a registration)

[125] Caralli, Richard A., James F. Stevens, Lisa R. Young and William R. Wilson, *The OCTAVE Allegro Guidebook, v1.0*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2007. https://www.cert.org/octave/allegro.html (under the download link, which requires a registration)

[126] Caralli, Richard A., James F. Stevens, Lisa R. Young and William R. Wilson, *Introducing OCTAVE Allegro: Improving the information security risk assessment process*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2007, p. 2. https://www.cert.org/archive/pdf/07tr012.pdf

[127] Alberts, Christopher J., and Audrey J. Dorofee, *OCTAVE*[SM] *Criteria, Version 2.0.*

	• RA 4 Generic threat profile • RA 5 Catalog of vulnerabilities
Defined process	• RA 6 Defined evaluation activities • RA 7 Documented evaluation results • RA 8 Evaluation scope
Foundation for a continuous process	• RA 9 Next steps • RA 3 Catalog of practices
Risk management principles	
Forward-looking view	• RA 10 Focus on risk
Focus on the critical few	• RA 8 Evaluation scope • RA 11 Focused activities
Integrated management	• RA 12 Organizational and technological issues • RA 13 Business and information technology participation • RA 14 Senior management participation
Organisational and cultural principles	
Open communication	• RA 15 Collaborative approach
Global perspective	• RA 12 Organizational and technological issues • RA 13 Business and information technology participation
Teamwork	• RA 1 Analysis team • RA 2 Augment analysis team skills • RA 13 Business and information technology participation • RA 15 Collaborative approach

Table 3.1

One of OCTAVE's core concepts is "Self Direction", which means that the entire evaluation must be conducted in-house by a multi-disciplinary, cross-functional team (the so-called "Analysis team") composed of employees of the organisation.

As an example, Figure 3.5 below shows the process of the first OCTAVE-based method (hereafter referred as the OCTAVE method).[128]

[128] OCTAVE-S is a three-phase process with a more formal structure than the OCTAVE method and uses only five processes. OCTAVE Allegro has four phases. It also has a more formal structure than the OCTAVE method and uses eight steps to complete.

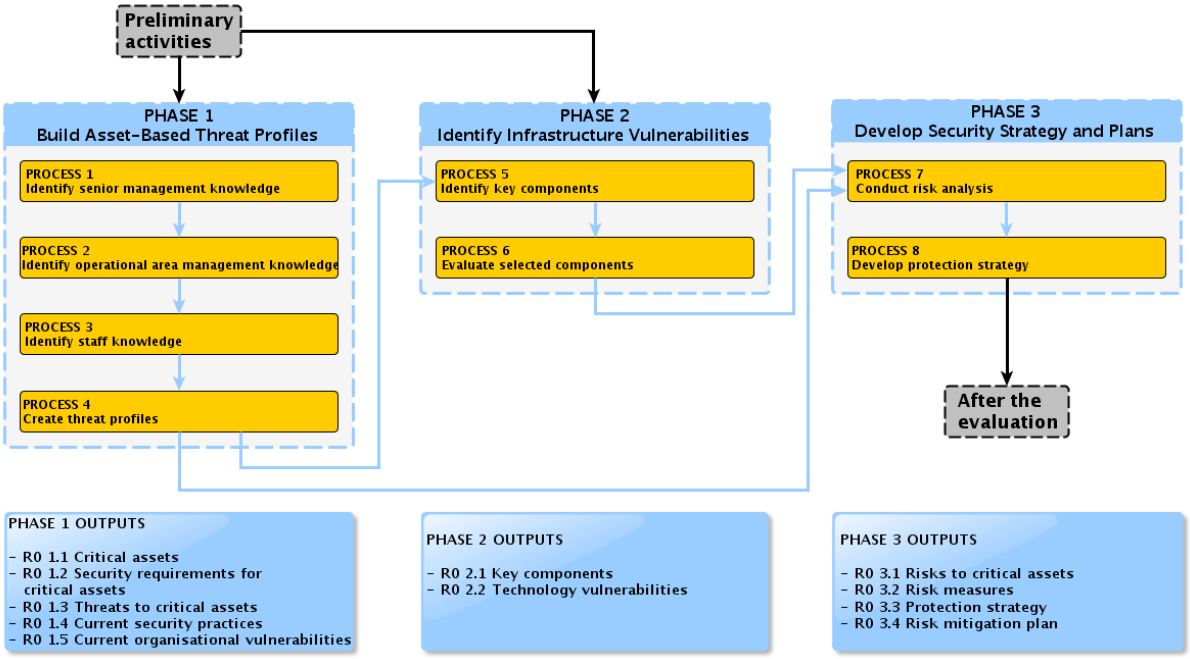


Figure 3.5: The OCTAVE method evaluation process

1. Phase 1 consists of the organisational evaluation. During progressive elicitation workshops spanning four processes, the analysis team gathers data from the management staff as well as from the technical staff. Each of them contributes their own views on what is important and what constitute the critical assets for the organisation, as well as what is currently done to protect those assets. Threats to the critical assets are also identified during this phase and threat profiles are built in the end.
2. Phase 2 consists of the technical evaluation. During two processes, the IT infrastructure is described, analysed and physically tested in order to identify its weaknesses.
3. Phase 3 is the last phase of the evaluation process. It spans two processes and consists of the risk analysis as well as the elaboration of various plans that include the protection strategy and the mitigation strategy.

As such, an OCTAVE-based method is not a full risk management method but rather a risk evaluation method that provides "a snapshot in time of the current information security risks of the organisation". Hence, an OCTAVE-based evaluation has clear limits, with start and end points. During such an evaluation, the analysis team performs the following activities:

- identifying the organisation's information security risks
- analysing those risks in order to determine the priorities
- planning the improvements in order to develop a protection strategy.

While implementing the controls, monitoring the implementation and checking for any deviation are left outside OCTAVE's overall process. In this regard, OCTAVE is not a full "Plan-Do-Check-Act" (PDCA)[129] process even if it includes some provisions for carrying out the missing activities as set out in the principle "Foundation for continuous improvement".

[129] Wikipedia. https://en.wikipedia.org/wiki/PDCA

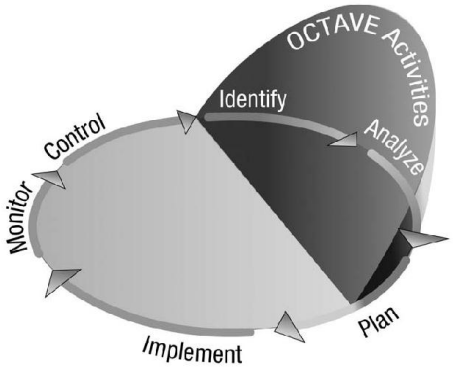


Figure 3.6: OCTAVE and Risk management activities[130]

Finally, thanks to the OCTAVE criteria, an OCTAVE-based method is quite flexible and includes some room for tailoring and for customisation. Examples of such tailoring can be found in "Applying OCTAVE: Practitioners Report".[131]

In the following, the analysis regarding the PIAs methodologies is mainly done against the OCTAVE method as it is the most flexible method of the three published by SEI.

	Touch points questions	Evidence from OCTAVE®
1	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	It includes provisions for taking into account the requirements set out in the relevant regulations. This is part of the "Tailoring process" within the "Preliminary activities" where, for instance, the "Catalog of practices" should be adapted to "to suit a particular domain's standard of due care or set of regulations"[132].
2	Is the RM methodology regarded as a process or is it simply about producing a report?	It is a risk evaluation process, providing a snapshot of the current information security risks of an organisation. Its final outputs are "Protection strategy" and "Risk mitigation plans", which then need to be implemented. It is not a full PDCA process running throughout a project lifecycle. However, it includes provisions for continuous improvements as set out in the Principle "Foundation for a continuous process" from which the Attribute "RA 9 Next steps" is derived. And it calls for running the evaluation on a regular basis and/or when changes occur in the organisation as the snapshots produced by the evaluation could quickly become outdated.
3	Does the RM methodology address	It is a general information security risk evaluation

[130] Alberts, Christopher J., and Audrey J. Dorofee, *OCTAVE[SM] Criteria*, Version 2.0, p. 8.
[131] Woody, Carol, *Applying OCTAVE: Practitioners Report*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2006. https://www.cert.org/archive/pdf/06tn010.pdf
[132] Alberts, Christopher J., and Audrey J. Dorofee, *OCTAVE[sm] Method Implementation Guide Version 2.0 Volume 2 Preliminary Activities*, Carnegie Mellon University, Pittsburgh, PA, 2001.
https://www.cert.org/octave/octavemethod.html (under the download link which requires a registration)

	Touch points questions	Evidence from OCTAVE®
	only information privacy protection or does it address other types of privacy as well?	method. It does not include specific provision for information privacy or other type of privacy.
4	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?	No. It has been designed with current and running systems in mind. As such it mainly concerns the operation and maintenance of a system's lifecycle. However, there are considerations[133] for expanding its use to the development phase in order to capture security requirements as early as possible.
5	Does the RM methodology place responsibility for its use at the senior executive level?	Yes. Senior management is required to participate as set out in the Attribute "RA 14 Senior management participation". In "Process 1", senior managers must contribute their views about what assets are important to them and need to be protected. In "Process 8", they must review, refine and approve the protection strategy and mitigation plans. In "Next steps", they must provide the necessary resources for the implementation and decide what to do next.
6	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	Yes. OCTAVE calls for development of plans and terms of reference as well as the organisation of the elicitation workshops for any evaluation as part of "Preliminary activities".
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	There is no direct provision for this. However, OCTAVE calls for adapting itself to the organisation's context. This includes (e.g.) adapting the "Catalog of practices" that can be fed with the results of an environment scan.
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	Yes. It can be tailored and adapted to the needs of each organisation. This should take place during "Preliminary activities".
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	Yes. The evaluation process is based on a progressive series of workshops, as set out in the Attribute "RA 15 Collaborative approach", where the relevant and necessary persons must participate. Senior managers and staff members from across the organisation must contribute their views to identify the critical assets, the security requirements, the possible threats and vulnerabilities, etc. While it makes clear provisions for internal participation, external participation is less evident but not excluded.
10	Does the RM methodology include provisions for putting in place measures to achieve clear	Yes. As set out in the Attribute "RA 15 Collaborative approach", the relevant and necessary persons must provide their views in

[133] Caralli, Richard A., James F. Stevens, Lisa R. Young and William R. Wilson, *Introducing OCTAVE Allegro: Improving the information security risk assessment process*, pp. 27-28

	Touch points questions	Evidence from OCTAVE®
	communications between senior management, the project team and stakeholders?	elicitation workshops. This includes staff members, senior management and the Analysis team.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	Yes. Risks to critical assets are identified during "Process 7" in Step 3. It corresponds to the Output "RO 3.1 Risks to Critical Assets", where critical assets can be anything from information, processes, equipment or even individuals.
12	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	Yes. This occurs during "Process 8" in Step 3. It corresponds to the Output "RO 3.4 Risk mitigation plan", where the Analysis team must create plans to reduce the risks to the organisation's critical assets.
13	Does the RM methodology include provisions for documenting the process?	Yes. The Analysis team is required to document fully the evaluation it carries out. This corresponds to the Attribute "RA 7 Documented evaluation results".
14	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?	No. There is no evidence about this.
15	Does the RM methodology call for a review if there are any changes in the project?	This is not directly part of it. However, provisions for continuous improvement are enshrined in the Principle "Foundation for a continuous process". In this regard, Attribute "RA 9 Next steps" includes recommendations for monitoring information security risks, for looking for new risks, and for possible changes to existing risks.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	It is an evaluation process that should be run on a regular basis, and that produces snapshots of the current security state of an organisation. There is no direct call for an audit. However, during the evaluation process, one of the outputs of the first phase is "RO 1.4 Current security practices", which can be regarded as a kind of audit result of the "Risk mitigation plans" of the previous run. Justification for not implementing some controls is in the "Protection strategy".

Conclusions and recommendations

OCTAVE-based methods are mainly risk evaluation methods, not full risk management methods. They have been designed for the USA regulation context to evaluate running systems and they do not include specific provision for privacy risk analysis unless those risks merge with information risks, which is often the case in the US. However, those methods are flexible enough to be tailored to various needs.

Regarding PIA methodology as set out in the ICO handbook, OCTAVE-based methods need the following enhancements:

- Clear provisions about how to use those methods in the design and development phases of systems
- Provisions for including external views during the consultation processes in order to include other types of stakeholders in addition to the organisation's staff
- Provisions for documents for public use at the end of the evaluation
- Provisions about how to extend the "Catalog of practices" with privacy requirements as set out in the regulation in the European area.

3.3.4 NIST SP 800-30 Guide for Conducting Risk Assessments

NIST is the National Institute of Standards and Technology, which comes under the auspices of the U.S. Department of Commerce. Its *Guide for Conducting Risk Assessments* (SP 800-30, 2012) deals with *Information Security* in an elaborate and systematic document that describes the risk assessment (RA) process in four steps: preparing for RA, conducting RA, communicating and sharing RA information, and maintaining the RA. NIST encourages organisations to use RA flexibly so that it can be integrated into broader processes of risk management. Thus, there are many choice and decision points, and the *Guide* is not deterministic even if its procedures are highly detailed. NIST issues a prudent cautionary note:

> Organizations are cautioned that risk assessments are often not precise instruments of measurement and reflect the limitations of the specific assessment methodologies, tools, and techniques employed—as well as the subjectivity, quality, and trustworthiness of the data used. Risk determinations may be very coarse due to the assessment approach selected, the uncertainty in the likelihood of occurrence and impact values, and the potential mischaracterization of threats. Risks that are on the borderline between bins using the organization-defined binning scales, must ultimately be assigned to one bin. This determination could have a significant effect on the risk prioritization process. Thus, organizations should incorporate as much information as practical on particular risks during the prioritization process to ensure that the values for risks are appropriately determined (e.g., very low, low, moderate, high, very high).

As information security is its focus, NIST's *Guide* is only somewhat aware of PIA and the protection of privacy in any wider sense, only mentioning PIA on one page and personally identifiable information (PII) on another; it does not clearly refer to privacy threats as such, especially outside the organisation. Nonetheless, there may be "touch points" with the PIA Handbook and "open doors" where PIA could be inserted into the RA process. NIST works with other entities to establish specific mappings and relationships between its security standards and guidelines, and those developed by the ISO/IEC.

The *Guide* sees RA as supporting enterprise-wide risk management towards dealing with the threats and vulnerabilities that beset information systems. Vulnerabilities may "compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by [information] systems". Threats "can include purposeful attacks, environmental disruptions, human/machine errors, and structural failures, and can result in harm to the national and economic security interests of the United States". They "can have adverse effects on organizational operations and assets, individuals, other organizations, and

the Nation" – a phrase that is repeated many times in the *Guide*, implicitly underlining the fact that the *Guide* does not consider other adverse effects or impacts (e.g., on privacy), and that the unspecified "individuals" concerned are likely to be those within the organisation itself. The purpose of RA is stated to be organisation-centred in its concerns, and the "impact (i.e., harm)" is indicated as "harm to organizations".

RAs are to be conducted at all tiers of an organisation: Tier 1 (organisation level), Tier 2 (mission/business process level), and Tier 3 (information system level). For the third tier, NIST's reference publication is the *Risk Management Framework* as seen in NIST Special Publication 800-37; NIST Special Publication 800-39 (described elsewhere in this report), which supersedes the present *Guide* as the primary source for guidance on information security risk management, is also referenced.

There are two main Chapters and supporting appendices. Chapter Two, the first one, introduces basic concepts (risk management process; RA). Risk management processes include:

- framing risk
- assessing risk
- responding to risk
- monitoring risk

and there are information and communication flows linking all of these. Organisations *frame* risk, establishing a risk context that describes the environment in which risk-based decisions are made. This leads to a *risk management strategy* that deals with how the organisation will assess, respond to and monitor risk. It also delineates the intra-organisational boundaries for risk-based decisions. Organisations then *assess* risk within the frame's context, in order to identify:

- threats to organisations (i.e., operations, assets, or individuals) or threats directed through organisations against other organisations or the nation
- vulnerabilities internal and external to organisations
- the harm (i.e., adverse impact) that may occur given the potential for threats exploiting vulnerabilities
- the likelihood that harm will occur.

This results in a *determination of risk*, a function of the degree and the likelihood of harm. The *Guide* notes that "[o]rganizational vulnerabilities are not confined to information systems but can include, for example, vulnerabilities in governance structures, mission/business processes, enterprise architecture, information security architecture, facilities, equipment, system development life cycle processes, supply chain activities, and external service providers." It does not include personal data or personally identifiable information in this catalogue.

Next, risk management deals with the organisation's *response* to the determined risk. This aims at consistent response through

- developing alternative courses of action for responding to risk
- evaluating the alternative courses of action
- determining appropriate courses of action consistent with organisational risk tolerance
- implementing risk responses based on selected courses of action.

Monitoring is the fourth step, the purpose of which is to

- determine the ongoing effectiveness of risk responses (consistent with the organisational risk frame)
- identify risk-impacting changes to organisational information systems and the environments in which the systems operate
- verify that planned risk responses are implemented and that information security requirements derived from and traceable to organisational missions and business functions, federal legislation, directives, regulations, policies, standards, and guidelines are satisfied.

NIST 800-30 concentrates upon the *risk assessment* component. This is not a one-time activity but continues "throughout the system development life cycle and across all of the tiers in the risk management hierarchy". The *Guide* defines risk in a conventional manner as a function of the impact and the likelihood of a potential circumstance occurring. It outlines a *risk assessment methodology* that includes an explicit risk *model* and a qualitative or quantitative approach, an *analysis approach* that could be oriented towards threats, vulnerabilities or asset impacts. Organisations can use multiple methodologies depending on a variety of circumstances, but by making explicit what they are doing, they increase the *reproducibility* and *repeatability* of their RAs.

The *Guide* discusses *risk factors* that are defined by a risk model; these include threat, vulnerability, impact, likelihood and predisposing condition. These are each discussed at far greater length than can be summarised here, and are further disaggregated into a variety of sub-topics and taxonomies. The reflexivity of risk is reflected in the *Guide*'s interest in showing how threats can be *shifted* by adversaries who respond to the perceived safeguards and countermeasures that they seek to overcome. However, not all threats are attributable to adversaries seeking to attack a system's vulnerabilities: many threat sources are non-adversarial. The discussion of *impact* – the magnitude of harm – may be of particular interest for its identification of its causes, including

- unauthorised disclosure of information
- unauthorised modification of information
- unauthorised destruction of information
- loss of information or information system availability.

We can observe that at least the first three of these activities are within the scope of data protection and information privacy regulation, and the *Guide* – at this point only – edges into PIA territory by saying that an organisation's "security categorization levels indicate the organizational impacts of compromising different types of information. Privacy Impact Assessments and criticality levels (when defined as part of contingency planning or Mission/Business Impact Analysis) indicate the adverse impacts of destruction, corruption, or loss of accountability for information resources to organizations."

However, privacy is not grasped as a harm or specifically as an "organisational asset", which is defined as "high-impact programs, physical plant, mission-critical information systems, personnel, equipment, or a logically related group of systems. More broadly, organizational assets represent any resource or set of resources which the organization values, including intangible assets such as image or reputation."

On the other hand, the concept of "stakeholder" is represented in the *Guide*, when it says that "harm can be experienced by a variety of organizational and non-organizational stakeholders including, for example, heads of agencies, mission and business owners, information

owners/stewards, mission/business process owners, information system owners, or individuals/groups in the public or private sectors relying on the organization—in essence, anyone with a vested interest in the organization's operations, assets, or individuals, including other organizations in partnership with the organization, or the Nation."

Following its further development of concepts involved in risk models, the *Guide* outlines *assessment approaches*, including quantitative and qualitative assessments, and *analysis* approaches before discussing the effects of organisational culture on RAs: for example, in shaping the choice of qualitative or quantitative approaches. It next shows systematically the application of RAs at the three tiers of an organisation. Although it is not clear to which tier(s) a PIA would pertain, it could be argued that at the lowest – information system – tier, where the initiation of a new system is likely to be located, is an appropriate but not unique place to instigate a PIA in organisations of the kind to which the *Guide* relates.

In any case, RA activities are stated to be capable of integration with steps in NIST's Risk Management Framework, which are seen as:

- categorise (threats and vulnerabilities)
- select (security controls)
- implement (security controls)
- assess (risk)
- authorise (officials to take action)
- monitor (effectiveness of security controls; changes to information systems and their environments; compliance to laws and regulations, etc.).

Then follows a discussion of risk communication and information sharing, before Chapter Three describes the process of conducting an RA in terms of four steps:

- prepare for assessment
- conduct assessment
- maintain assessment
- communicate results.

Each of these steps is further unpacked in terms of separate tasks – again, these are too elaborate to be summarised – that put into practice what has already been described and categorised earlier in the *Guide*, and that are linked to further specification, templates, scales and tables contained in several appendices. Possible "touch points" are shown below:

	Touch point questions	**Evidence from NIST 800-30**
1	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	It mentions legislation but also includes "directives, regulations, policies, standards, and guidelines".
2	Is the RM methodology regarded as a process or is it simply about producing a report?	This is a process.
3	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?	It does not deal with privacy, but where it mentions it, it is with reference to personally identifiable information only. This could perhaps be done within the

		scope of the RA, but adopting a conception of privacy that went beyond information *security* would be a prerequisite for the organisation.
4	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?	RA is conducted at the stage of initiating a project and continuously thereafter, and will be influential over the course of its development.
5	Does the RM methodology place responsibility for its use at the senior executive level?	This RA involves responsibilities (activities) at several levels.
6	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	It is not clear that this RA develops a plan and terms of reference as such, although this is implicit. It indicates consultations on specific matters: "Mission/business owners and mission/business subject matter experts can be consulted to obtain the most complete and up-to-date information on mission/business impacts [regarding today and the future]. Other subject matter experts or stakeholder representatives can be consulted to obtain information on immediate versus future impacts (e.g., consulting the Privacy Office for impacts to individuals)."
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	It mentions many other NIST risk, security and other publications, as well as ISO and other standards.
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	This scale does not seem to apply to the RA, except perhaps in terms of *risk aggregation*, which "roll[s] up several discrete or lower-level risks into a more general or higher-level risk. Organizations may also use risk aggregation to efficiently manage the scope and scale of risk assessments involving multiple information systems and multiple mission/business processes with specified relationships and dependencies among those systems and processes."
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	Stakeholders are mentioned in a few places, for example, with reference to information sharing and communication, where they are "e.g., mission/business owners, risk executive [function], chief information security officers, information system owners/program managers". Undefined "stakeholder representatives"

		are mentioned in connection with consultation over impacts. Stakeholders are also described as those harmed by unauthorised information disclosure, etc.: "a variety of organizational and non-organizational stakeholders including, for example, heads of agencies, mission and business owners, information owners/ stewards, mission/business process owners, information system owners, or individuals/ groups in the public or private sectors relying on the organization—in essence, anyone with a vested interest in the organization's operations, assets, or individuals, including other organizations in partnership with the organization, or the Nation." Stakeholders are to be consulted early, and it is implied that their perspectives should be considered.
10	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	Yes, but not explicitly regarding stakeholders.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	This RA is almost exclusively non-individual in focus.
12	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	Alternative actions to mitigate risk are mentioned as part of assessment procedures, but not concerning privacy impact.
13	Does the RM methodology include provisions for documenting the process?	Documentation is extensively covered in the appendices for different tasks.
14	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?	Nothing is mentioned beyond the communication of the results of the RA internally within the organisation.
15	Does the RM methodology call for a review if there are any changes in the project?	Continuous monitoring is important to this RA.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	Review of risk management decisions is part of *maintaining* this RA.

Conclusions and recommendations

NIST 800-30 provides highly detailed and comprehensive RA methods that currently do not focus on privacy or impacts and harms to individuals whose personal data are processed in the information systems in question, the security of which is paramount as the *Guide*'s rationale. Information security might tangentially protect individual information privacy or the privacy of groups and categories and persons. There may, however, be "open doors", "touch points" and other affordances in NIST 800-30 and in the PIA Handbook that could be worth developing. There is already mention of PIA, albeit focused on impact on the organisation, but this could perhaps be cultivated towards including impact on individuals as well. Given that there is also mention of the involvement of an organisation's Privacy Office in internal consultation about impacts on individuals, this could provide the "open door" for conduct of a PIA. In addition, the accepted routine of identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts could provide an opening for inserting privacy protections and design solutions (PbD; PETs). The internal communications processes should be extended to stakeholders as well if PIA were inserted into the RA, especially as this methodology has an all-embracing definition of "stakeholders" that includes external individuals or their representatives.

3.4 PRIVACY RISK MANAGEMENT

3.4.1 ISO/IEC 29100:2011 Information technology — Security techniques

This standard provides a framework for protecting personally identifiable information (PII).[134] It defines PII as any information that can be used to identify a PII principal (a person or a "data subject", to use EC terminology) or that might be linked to a PII principal, either directly or indirectly. It defines privacy principles in terms of PII, so the standard does not address all types of privacy. Organisations can use the framework to help define their "privacy safeguarding requirement". The framework describes such requirements and lists privacy principles based on other well-known guidance documents. The standard can also support other privacy standardisation activities, such as privacy risk assessments and controls.

The standard comprises five sections, one annex and a bibliography. Section 2, on definitions, includes an interesting note that equates a privacy impact assessment with a privacy risk assessment, which it defines as the "overall process of risk identification, risk analysis and risk evaluation with regard to the processing of personally identifiable information". The definition does not include stakeholder consultation or even finding solutions to privacy risks.

Section 4 focuses on the basic elements of a privacy framework. It discusses actors and roles, interactions, recognising PII, privacy safeguarding requirements, privacy policies and controls. It identifies four types of actors involved in processing PII, namely, the PII principals, controllers, processors and third parties. It says a privacy principal does not always have to be identified by name. These different actors (stakeholders) can interact with each other in a variety of ways. The standard includes a table with several different scenarios showing possible information flows between the PII stakeholders (actors). It clarifies how information can be considered PII, e.g., if the information has an identifier that refers to a

[134] International Organization for Standardization (ISO), *Information technology – Security techniques – Privacy framework, ISO/IEC 29100:2011, First edition*, Geneva, 15 Dec 2011.

person, and it regards as PII any information that distinguishes one person from another (e.g., biometric data). The standard makes the point that it may be possible to identify someone even if there is no single attribute that uniquely identifies her. A combination of two or three or more attributes may be enough uniquely to identify the person. Table 6.2 provides a long list of example attributes that can be used to identify a person.

Privacy safeguarding requirements may arise whenever an organisation processes PII – e.g., in the collection, processing and storage of PII and in the transfer of PII to others, including others in third countries. The standard encourages organisations to identify privacy safeguarding requirements whenever they design an ICT system that will be used to process PII. It says the privacy risk management process comprises five main elements:

- establishing the context
- assessing risks
- treating risks
- communications and consultation
- monitoring and reviewing risks and controls.

At this point, the standard refers again to PIA, which it describes as that part of risk management that focuses on ensuring compliance with legislation and assessing the privacy implications of any new or modified programs. It says that privacy safeguarding requirements and PIAs should be part of the organisation's risk management framework, and describes privacy risk management as a process. That process should take into account various factors, including legal and regulatory, contractual, business, and others. Among the other factors are the privacy preferences of PII principals. The standard indirectly refers to "privacy by design" (PbD) when it says that ICT system designers should take into account the likely privacy preferences of the PII principals. Organisations should respond to the privacy safeguarding requirements with a set of privacy controls as an outcome of their privacy risk assessment and treatment. The controls should be embedded in the organisation's approach to PbD and in its information security management framework. The standard also says that top management should be involved in the establishment of the organisation's privacy policy. Distinguishing between an internal and an external privacy policy, the standard says that the organisation should document the controls used to enforce the policy.

Section 5 provides a list of privacy principles that were abstracted from those promulgated by various countries and international organisations. It says the privacy principles are to guide the design, development and implementation of privacy policies and controls. ISO 27005 formulates 11 privacy principles, as follows:

- *Consent and choice* means the PII principal must have a freely given, specific and knowledgeable choice (opt-in) about the processing of her PII. A PII principal should be able withdraw her consent without penalty.
- *Purpose legitimacy and specification* means ensuring that the purpose(s) complies with applicable law, and communicating the purpose with the PII principal before the organisation collects the information.
- *Collection limitation* means limiting the collection of PII to that which has a legal basis and to not more than necessary for the specified purpose(s). The standard says organisations should justify and document the PII they collect.
- *Data minimisation* means minimising the PII processed and the number of people who have access to such data.

- *Use, retention and disclosure limitation* means a limit to that necessary to fulfil specific, explicit and legitimate purposes, and retaining such data only as long as necessary to meet the specified purpose.
- *Accuracy and quality* mean that the data controller must ensure that the PII is accurate and relevant for the specified purpose.
- *Openness, transparency and notice* mean that the data controller should provide PII principals with clear and easily accessible information about its policies, procedures and practices in regard to the processing of PII. The data controller should also inform the PII principals about who might be provided with the PII and whom they can contact at the controller's address if they have questions or want to access their data.
- *Individual participation and access* means enabling the PII principals to access, review and correct their PII, provided their identity is authenticated.
- *Accountability* means that the organisation should document and communicate to stakeholders its privacy policies and practices. It also means that someone in the organisation is held responsible for implementing the privacy policies and practices. If the organisation transfers PII to a third country, it must ensure by means of contractual arrangements, for example, that the recipient will provide comparable privacy protection. If there is a data breach, the organisation must inform the relevant stakeholders about the breach and what it is doing to resolve it. Accountability also means there must be redress procedures in place.
- *Information security* means protecting PII to ensure its integrity, confidentiality and availability, and protect it against unauthorised access, use or loss.
- *Privacy compliance* means ensuring that the processing meets data protection and privacy safeguards (legislation and/or regulation), and enabling the conduct of audits. It also means that the organisation should conduct privacy risk assessments to ensure, among other things, that the organisation complies with laws and regulations and safeguarding requirements.

	Touch point questions	**Evidence from ISO 29100:2011**
1	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	Yes, it says controllers should be aware of all legal and regulatory requirements (section 4.5.1).
2	Is the RM methodology regarded as a process or is it simply about producing a report?	Section 4.5 on privacy safeguarding requirements refers to the privacy risk management process. A note also refers to PIA, which is a process.
3	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?	This standard is focused on personally identifiable information (PII).
4	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?	Not exactly, but it does say that the design of any ICT system involving the process of PII should be preceded by an identification of the relevant privacy safeguarding requirements.
5	Does the RM methodology place responsibility for its use at the senior executive level?	Yes, section 4.6 says the top management should be involved in establishing a privacy policy.
6	Does the RM methodology call for	No, it does not talk about developing a plan

	Touch point questions	Evidence from ISO 29100:2011
	developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	or terms of reference. It does, however, refer to consultation with stakeholders in section 4.5.
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	It says privacy risk management involves establishing the context (section 4.5).
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	No.
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	It refers to consulting interested parties and obtaining consensus.
10	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	It refers to communicating with PII principals and others.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	It refers to identification of PII risks from the perspective of the organisation.
12	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	Yes, it calls protection measures "privacy safeguarding requirements".
13	Does the RM methodology include provisions for documenting the process?	Yes, section 4.6 says the organization should document its privacy policy (both internal and external policies). It also says privacy controls should be documented. At section 5.4, it says organisations should document the type of PII collected as well as the justification for doing so.
14	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?	Not specifically, although it does mention communicating with stakeholders. Further, one of the privacy principles focuses on openness, transparency and notice. There, it says the organization should provide stakeholders with clear information about its PII policies and practices, the purpose for which it is processing PII, how to contact the controller, the choices open to PII principals, access to their data, the

	Touch point questions	Evidence from ISO 29100:2011
		possibility for correcting inaccurate data, etc.
15	Does the RM methodology call for a review if there are any changes in the project?	It says that privacy controls should be reviewed and reassessed periodically as part of an ongoing security risk management process (section 5.11). It also says, in regard to privacy safeguarding requirements, that the privacy risk management process should include monitoring and review and improving the process.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	Regarding its privacy principle regarding privacy compliance, the standard says the organisation should conduct audits (using either internal auditors or third party auditors) of the way in which it processes PII and its privacy safeguarding requirements. With regard to information security, it refers to the use of audits for discovering risks and vulnerabilities.

Conclusions and recommendations

ISO29100 is not a privacy risk management methodology *per se*, so it is a bit unfair to assess it as such. Its primary focus and value is on privacy terminologies and, especially, privacy principles. In section 5, wherein the privacy principles are identified and discussed, there is operational guidance, as the foregoing indicates. It has many "touch points" in common with the ICO PIA Handbook. As it is not, strictly speaking, a risk management methodology or process, it offers no "open doors" wherein a PIA could be conducted. However, it does refer to the privacy risk management process (notably in the section dealing with privacy safeguarding requirements) wherein there are "open doors", e.g., in regard to establishing the context, assessing and treating risks, communicating and consulting with stakeholders, and monitoring and review.

3.4.2 NIST SP 800-122, Guide to Protecting the Confidentiality of PII

NIST Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*[135] of April 2010 sketches the procedural steps and topics for PIA as a way of addressing confidentiality risks and applying safeguards. It cites much OMB (Office of Management and Budget) material on PIA. Its audience are a host of organisational personnel including security officers, privacy officers, privacy advocates and privacy support staff.

The *Guide* has many affinities with PIA and already builds PIA into its guidance, as PIA is mandated for US Federal information-processing projects having certain characteristics, and as guided by OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy*

[135] http://csrc.nist.gov/publiations/nistpubs/800-122/sp800-122.pdf

Provisions of the E-Government Act of 2002.[136] NIST's *Guide*, as a computer security document, addresses itself to data breaches and the breaches of confidentiality that these may cause, but it is closely aligned to the protection of privacy although privacy intrusion is not indicated as a confidentiality harm. The invocation of the Privacy Act of 1974, of Fair Information Practices (FIPs) and of PIA, all contribute to a view that this document is about privacy protection as much as it is about preventing and responding to breaches of confidentiality. Whereas European information privacy and data protection legislation uses the term "personal data", the *Guide* adopts the American term "PII", which it defines (taking it from a Government Accountability Office (GAO)'s reinterpretation of OMB usage) as: "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." Appendix C shows 11 alternative terms for PII as used in a variety of US laws and OMB memoranda.

The 59-page *Guide* comprises an Executive Summary, an Introduction, and Introduction to PII, and chapters on PII Confidentiality Impact Levels, PII Confidentiality Safeguards, Incident Response to Breaches Involving PII, and seven appendices. The *Guide* shows how to determine whether PII is at stake, and gives many examples. In identifying PII, an organisation is required to use "privacy threshold analyses" (PTAs), also known as "initial privacy assessments" (IPAs). It notes that some agencies require a PTA to be completed before a new information system is implemented or where there is a substantial change to an existing system: "PTAs are used to determine if a system contains PII, whether a Privacy Impact Assessment (PIA) is required, whether a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system." Appendix A gives some scenarios for PII identification and handling. The *Guide*'s closeness to a PIA process is illustrated in this phase.[137] It then invokes the customary OECD Privacy Guidelines,[138] or FIPS: Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, Accountability; these are elaborated in Appendix D. Clarifying its understanding of the relationship between privacy and confidentiality, and justifying the reference to FIPs, the *Guide* says:

> Privacy is much broader than just protecting the confidentiality of PII. To establish a comprehensive privacy program that addresses the range of privacy issues that organizations may face, organizations should take steps to establish policies and procedures that address all of the Fair Information Practices. For example, while providing individuals with notice of new information collections and how their personal information will be used and protected is central to providing individuals with privacy protections and transparency, it may not have a significant impact on protecting the confidentiality of their personal information. On the other hand, the Fair Information Practices related to establishing security safeguards, purpose specification, use limitation, collection limitation, and accountability are directly relevant to the protection of the confidentiality of PII. As a result, these principles are highlighted throughout this document as appropriate.

The determination of PII confidentiality impact levels is a key feature in the process, in which (quoting legislation), "[t]he security objective of confidentiality is defined by law as

[136] http://www.whitehouse.gov/omb/memoranda/m03-22.html
[137] The *Guide* cites PTA/IPA templates, at: http://www.usdoj.gov/opcl/initial-privacy-assessment.pdf or http://www.dhs.gov/xlibrary/assets/privacy/privacy_pta_template.pdf.
[138] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980.

'preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information'". NIST's Risk Management Framework[139] is recommended as a way of determining impact levels, which differ from the confidentiality impact levels elsewhere described in federal information security standard documents by including additional PII considerations. The impact levels denote harms: "any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII". An illustrative list of harms to the individual ("any negative or unwanted effects") does not, however, mention privacy. The levels to be determined are Low, Moderate, or High, and these are illustrated with examples. The factors to be examined in determining levels are:

- Identifiability
- Quantity of PII
- Data field sensitivity
- Context of use
- Obligation to protect confidentiality
- Access to and location of PII.

Examples are given of how these should be used. But it is not clear whether these are *impact* factors or *likelihood* factors, or a combination; in other words, how they relate to risk-management analysis. The *Guide* next turns to PII confidentiality safeguards, identifying several categories and subtypes:

- Operational safeguards
    - policy and procedure creation
    - awareness, training, and education
- Privacy-specific safeguards
    - minimising the use, collection, and retention of PII
    - conducting privacy impact assessments
    - de-identfying information
    - anonymising information
- Security controls
    - (17 subtypes).

Focusing on PIA – "structured processes for identifying and mitigating privacy risks, including risks to confidentiality, within an information system" – the *Guide* quotes an OMB source[140] and says that "a PIA should address confidentiality risks at every stage of the system development life cycle". It notes that many organisations have their own PIA templates, but that some topics are commonly addressed:

- What information is to be collected
- Why the information is being collected
- The intended use of the information
- With whom the information will be shared
- How the information will be secured
- What choices the agency made regarding an IT system or collection of information as a result of performing the PIA.

[139] http://csrc.nist.gov/groups/SMA/fisma/framework.html
[140] OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. http://www.whitehouse.gov/omb/memoranda/m03-22.html.

Incident response, in case there is a data breach that threatens confidentiality, requires its own routines, but "often requires close coordination among personnel from across the organization, such as the CIO, CPO, system owner, data owner, legal counsel, and public relations officer. Because of this need for close coordination, organizations should establish clear roles and responsibilities to ensure effective management when an incident occurs." This hints at internal communication within the organisation, and also requires "incident response plans" to handle breaches involving PII. Referring to NIST SP 800-61 Revision 1,[141] the *Guide* extends to the case of PII involvement the security-incident response's four phases: preparation; detection and analysis; containment, eradication recovery; and post-incident activity.

Among the appendices, Appendix B has frequently asked questions, including one about PIA and when it has to be conducted. It points out that the E-Government Act 2002 requires Federal agencies to do a PIA under the following circumstances:

- Developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
- Initiating a new collection of information that—
    - Will be collected, maintained, or disseminated using information technology; and
    - Includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the federal government.

It points out that OMB Memorandum 03-22 provides examples of system changes that create new privacy risks and trigger the requirement for a new PIA:

- Conversions—when paper-based records are to be converted to electronic systems
- De-Identified to Identifiable—when functions applied to an existing information collection change de-identified information into information in identifiable form
- Significant System Management Changes—when new uses of an existing information system, including application of new technologies, significantly change how information in identifiable form is managed in the system
- Significant Merging—when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases, or otherwise significantly manipulated
- New Public Access—when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an information system accessed by members of the public
- Commercial Sources—when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources
- New Interagency Uses—when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives
- Internal Flow or Collection—when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form

[141] NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*. http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

- Alteration in Character of Data—when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

Finally, the *Guide* makes it clear that the E-Government Act 2002 requires PIAs to be published (with national security or "sensitive information" exemptions), and that a PIA report must analyse and describe the following aspects of an information system:

- What information is to be collected
- Why the information is being collected
- The intended use of the information
- With whom the information will be shared
- What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent
- How the information will be secured
- Whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a
- What choices the agency made regarding an information system or collection of information as a result of performing the PIA.

	Touch point questions	**Evidence from NIST SP 800-122**
1	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	Compliance with the Privacy Act 1974.
2	Is the RM methodology regarded as a process or is it simply about producing a report?	It is a process. There is no mention of producing an RM report separate from a PIA report.
3	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?	Only information privacy protection.
4	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?	Yes.
5	Does the RM methodology place responsibility for its use at the senior executive level?	Yes, but not exclusively.
6	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	Planning is only mentioned with regard to incident response. No consultation is mentioned.
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	No.

	Touch point questions	Evidence from NIST SP 800-122
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	The designation of impact levels perhaps relates to this.
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	There is no mention of stakeholders.
10	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	At one point in the discussion of incident response.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	Yes. It is concerned with both.
12	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	The chapter on safeguards deals with these, but not the justification of the business need.
13	Does the RM methodology include provisions for documenting the process?	Not clearly in the RM methodology, but probably indicated for any accompanying PIA.
14	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?	No, because no such report is envisaged as a result of the risk management processes for confidentiality, although where a PIA is conducted under federal regulations as an ancillary process, publication is required.
15	Does the RM methodology call for a review if there are any changes in the project?	As indicated in the PIA steps, changes trigger a PIA.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?	No.

Conclusions and recommendations

This *Guide* comes close to being a PIA approach, and there are several touch points with the PIA Handbook. On the other hand, there are many places where the full requirements of such a PIA are not indicated in this *Guide*, but insofar as they may be covered by PIA requirements

in the USA – the latter are not completely reproduced in this document – they are expected to be present in the situations envisaged by this *Guide*. There appear to be a number of "open doors" for the integration of PIA with such an approach to safeguarding the confidentiality of PII in the face of possible breaches. It might be difficult, however, to graft a "stakeholder" approach onto this.

3.4.3 CNIL methodology for privacy risk management

Methodology for privacy risk management[142] and *Measures for the privacy risk treatment*[143] are the English translations of two guides published by the French Data Protection Authority, the Commission Nationale de l'Informatique et des Libertés (CNIL)[144], *Guide – Gérer les risques sur les libertés et la vie privée*[145], for the former, and *Guide – Mesures pour traiter les risques sur les libertés et la vie privée*[146], for the latter. Both French guides were released in June 2012, while their English counterparts were released a bit later, in November 2012.

The first English document, of 31 pages, describes the method for managing risks. It comprises two chapters. The first one is more theoretical and explains the risk management concepts, while the second one is more practical and describes the methodology itself. Finally, four appendices supplement this guide, one of which describes possible threats that may jeopardise confidentiality, integrity and availability of personal data. The second English document, of 92 pages, is mainly a catalogue of good practices intended to treat risks. It comprises five chapters. The first four chapters describe controls that act on the elements part of a risk: the primary assets, the impacts, the source of risk and the supporting assets. The last chapter describes cross-organisational actions.

These two documents are a kind of follow-up to a first guide published in French in 2010 and translated into English in 2011, entitled *Guide – Security of personal data*.[147] While this first guide, of 40 pages, is "only" a catalogue of 17 fact sheets, the last two guides go one step further and provide "a complete analytical approach for improving the management of processing of personal data". They should be seen as tools to help data controllers to address the requirements set out in Article 34 of the Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties[148] (hereafter referred to as the French law for personal data protection) which requires data controllers to "take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the

[142] CNIL, *Methodology for privacy risk management*, CNIL, Paris, 2012.
http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf
[143] CNIL, *Measures for the privacy risk treatment*, CNIL, Paris, 2012.
http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Measures.pdf
[144] http://www.cnil.fr
[145] CNIL, *Guide - Gérer les risques sur les libertés et la vie privée*, CNIL, Paris, 2012.
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf
[146] CNIL, *Guide - Mesures pour traiter les risques sur les libertés et la vie privée*, CNIL, Paris, 2012.
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_securite_avance_Mesures.pdf
[147] CNIL, *Guide - Security of personal data*, CNIL, Paris, 2011.
http://www.cnil.fr/fileadmin/documents/en/Guide_Security_of_Personal_Data-2010.pdf . The French original version is entitled "Guide - La sécurité des données personnelles".
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf .
[148] CNIL, Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties, Paris, October 2011, http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf

data".[149]

The methodology described in *Methodology for privacy risk management* (hereafter referred to as CNIL's methodology) is based on the French risk management methodology EBIOS.[150] However, while EBIOS addresses information security as a whole, CNIL's methodology only focuses on privacy and takes into account the requirements set out in the French law for personal data protection. As such, CNIL's methodology appears as a kind of customised version of EBIOS that tries to make things as simple as possible as well as to focus on the essentials. As a result, some parts of EBIOS do not appear in CNIL's methodology, either because they are hidden and considered as implicit, or because they have been removed to lower the burden of carrying out such a privacy risk analysis.

Like EBIOS, CNIL's methodology uses an analytical approach to identify and then treat privacy risks. According to CNIL's methodology, a risk can be seen as a scenario describing how sources of risk might exploit the vulnerabilities of supporting assets leading to an incident on "primary assets" with, as a result, impacts on privacy.

As a dedicated method for privacy risk analysis, CNIL's methodology derives its "primary assets" directly from the requirements set out by the French law for personal data protection. Among them are legal processes the aim of which is to:

- inform data subjects (Article 32)
- obtain their consent if appropriate (Article 7)
- allow the exercise of the rights of opposition (Article 38)
- allow the exercise of the rights of access (Article 39)
- allow the exercise of the rights of correction and deletion (Article 40).

Organisations must also guarantee the confidentiality, integrity and availability of personal data. Possible sources of risk include one or more of the following three categories:

- Insiders: person who belong to the organisation
- Outsiders: persons from outside the organisation
- Non-human sources like computer viruses, natural disasters, etc.

"Supporting assets" may include: hardware, software, people, paper media and paper channel transmission.

Like EBIOS, CNIL's methodology is a five-step process that comprises:

- a background study, in order to identify the context of the processing of the personal data as well as to gain a view of the scope under consideration
- a feared events study, in order to obtain a detailed and prioritised list of all feared events that may affect the processing operation under consideration
- a threats study, in order to obtain a detailed, prioritised list of all threats that may allow feared events to occur
- a risk study, in order to obtain a risk map in order to determine the order in which they should be treated
- a measures study, in order to identify the necessary controls to treat the risks.

Unlike EBIOS, this process is clearly a recurring one, as shown on Figure 3.7.

[149] Ibid,. p. 26
[150] See section 6.3.2 above.

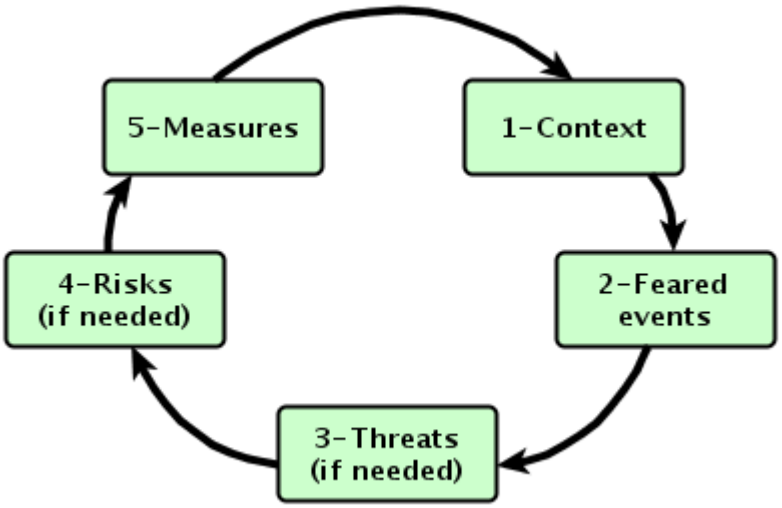


Figure 3.7: CNIL's methodology five steps cycling process[151]

Finally, CNIL's methodology claims to be fully compliant with international standards such as ISO 31000. Possible "touch points" are noted below:

	Touch points questions	Evidence from CNIL's methodology for Privacy Risk Management
1	Does the RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?	Yes. During its first step, which concerns context analysis, it calls for identifying all of the relevant guidelines to be followed. This includes regulations, sectoral requirements, etc.
2	Is the RM methodology regarded as a process or is it simply about producing a report?	It is described as a continuous improvement process, based on the well-known "Plan-Do-Check-Act"[152] (PDCA) process. It requires a continuous monitoring of any changes within the context, feared events, threats, risks and measures, as well as the necessary updates as soon as significant changes occur.
3	Does the RM methodology address only information privacy protection or does it address other types of privacy as well?	It addresses the risks to information privacy as well those arising to human identity, human rights, privacy as well as individual or public liberties.
4	Does the RM methodology say that it should be undertaken when it is still possible to influence the development of the project?	Yes. It makes evident provisions for starting the analysis as soon as a new processing operation is designed in order to optimise the costs of implementing the necessary and sufficient controls. In addition, Action 5.4, "Integrating privacy protection in projects", of the Cross-organisational actions section of the Catalogue, calls for integrating "the

[151] This drawing is based on the figure found in CNIL, *Methodology for privacy risk management*, p. 9.
[152] Wikipedia: https://en.wikipedia.org/wiki/PDCA

	Touch points questions	Evidence from CNIL's methodology for Privacy Risk Management
		protection of personal data in all new processing operations".
5	Does the RM methodology place responsibility for its use at the senior executive level?	It is particularly targeted at the data controller, who is often placed at a senior executive level. It also clearly states that "the validation of how risks have been handled as well as the acceptance of residual risk (remaining risks after application of measures), are part of the controller's responsibility".
6	Does the RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?	No. There is little or no direct evidence about any plan or terms of reference. However, as it is based on EBIOS, this aspect should be considered implicit. The same remark goes for the consultation strategy.
7	Does the RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?	Yes. During the context analysis[153] (the first step), it calls for gaining a clear view of the scope under consideration by identifying all of the useful information for risk management.
8	Does the RM methodology include provisions for scaling its application according to the scope of the project?	Not directly. It describes itself as a "complete analytical approach for improving the management of processing of personal data". As such, it may not be appropriate for all situations, and in some cases it should be adapted. However, as this methodology is based on EBIOS, the scaling process should be considered implicit.
9	Does the RM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?	While it calls for consulting the relevant internal stakeholders, there is no explicit provision for consulting external ones. However, in step one "Context analysis", it calls for identifying the main benefits of the risk management to the data subjects as well as to the whole organisation.[154]
10	Does the RM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?	No. There is little or no evidence about any communication plan. However, as it is based on EBIOS, this aspect should be considered implicit. Further, Action 5.3, "Managing the privacy protection policy", of the Cross-organisational actions section of the Catalogue, calls for "a documentary base

[153] CNIL, *Methodology for privacy risk management*, pp. 10-11.
[154] Ibid., p. 11.

	Touch points questions	Evidence from CNIL's methodology for Privacy Risk Management
		setting out data protection objectives and rules"[155] adapted to each communication target.
11	Does the RM methodology call for identification of risks to individuals and to the organisation?	It focuses specifically on the risks arising if the requirements of the French law for personal data protection are not met. This includes only the risks arising to individuals.[156] However, by addressing those kinds of risk, the organisation also addresses other types of risk, including some relevant to the organisation.
12	Does the RM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?	Yes. This is done in step five "Measures study", which aims to build the protection system. This is an iterative process where controls are added until the level of risk is considered as acceptable.
13	Does the RM methodology include provisions for documenting the process?	Yes. Each of the five steps must be fully documented and explanations for the choices made must be given.
14	Does the RM methodology include provision for making the resulting document public (whether redacted or otherwise)?	No. There is no evidence about the public release of any document.
15	Does the RM methodology call for a review if there are any changes in the project?	Yes. If any changes appear within the context, feared events, threats, risks or measures, it calls for a review as well as the necessary updates. This is clearly indicated in step one, "Context analysis", as well as in step five, "Measures", where CNIL reminds the reader that the measures must be continually improved. In addition, Action 5.5, "Supervising privacy protection", of the Cross-organisational actions section of the Catalogue, calls for regularly inspecting personal data processing as well as the effectiveness and the appropriateness of the planned controls.
16	Does the RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification	Yes. In step five, "Measures", it makes provisions for the implementation of the necessary protective measures as well as their regular audit. It also indicates that if any residual risks should be accepted (which is

[155] CNIL, *Measures for the privacy risk treatment*, p. 78.
[156] CNIL, *Methodology for privacy risk management*, p. 5.

	Touch points questions	Evidence from CNIL's methodology for Privacy Risk Management
	for not implementing some recommendations?	still possible if the benefits of the treatment are greater than the risks), then clear explanations should be given.

Conclusions and recommendations

CNIL's methodology is a dedicated methodology for privacy risk management arising if the requirements set out by the French law for personal data protection are not met. The methodology was written and is maintained by a Data Protection Authority. As such, it seems particularly suitable for PIAs. However, when compared with the PIA process, it seems possible to enhance some points:

- Consultation with external stakeholders is not explicitly set out in CNIL's methodology; this should be added when appropriate.
- There is no provision for releasing a public report describing the treatment, its objectives, the results of the risk analysis and the controls identified and implemented to lower (if not remove) those risks. This should be added as well.

Finally, other points appear to be hidden in CNIL's methodology while they do exist in EBIOS, from which it is derived. Those points are mainly organisational and concern the terms of reference for the risk analysis, communication with relevant stakeholders, as well as the scaling process for the study, which could be described and explained more explicitly.

3.5 PRACTICAL APPROACHES FOR INTEGRATING PRIVACY RISKS INTO RISK MANAGEMENT METHODOLOGIES AND STANDARDS ADOPTED BY RESPONDENTS

This section, as with our previous discussion in section 2.4, highlights our findings from the January 2013 survey on the most adopted "open doors" for integrating privacy risks into adopted risk management standards and methodologies, based on the responses received. Rather than providing an exhaustive list of "open doors", this section summarises the most adopted "open doors" for integrating privacy risks into adopted risks management standards, based on the responses received. This summary could provide useful directions for achieving practical integration.

From the survey and case studies analysis, the findings indicate that some critical point of integration, or "open doors", related to risk approaches and processes, which are discussed below (e.g., corporate policies and risk governance arrangements and frameworks), need to be in place for additional integration to happen. Therefore, we could regard the integration of privacy risk and PIA into the risk management processes as a necessary pre-condition for achieving an effective integration of privacy risk and PIA into project management processes.

We have organised the "open doors" for risk management standards and processes around two categories: at *the risk corporate level*, and at *the single-risk project level*. The corporate level refers to the integration of privacy risks and PIA into overreaching, macro corporate frameworks, while the single risk project level indicates operational integration at the micro, individual project level.

Risk corporate level "open doors"

- *Corporate compliance standards and policies*: This concerns the formal inclusion of privacy risks and the need to do PIAs into internal, corporate compliance standards and policies. Once privacy risks and PIA processes become a corporate policy and/or standard, all employees, outsourcing providers and contractors must comply with the policy and/or standard.
- *Incorporation of privacy risk into corporate risk registers and category of risks.* This refers to the inclusion of identified privacy risks into the appropriate service, department or corporate risk register. Often, as one of the respondents stated: "The organisation's Corporate Risk Register includes a specific risk on Information Management which includes security and privacy of information and this is regularly reviewed through the risk management process." Usually, within the corporate information risk register, information risk management disaggregates the risks into data protection, freedom of information, information security, records management, and data quality. Mitigation plans are often also part of the register. Once the risks are placed on the registers, they are managed either through standard project management (for projects) or risk management processes (service, department, corporate risks).
- *Annual compliance risk assessment:* Some organisations perform annual compliance risk assessments, which formally include privacy risks, on business-critical applications and organisational functions, using the organisation's adopted risk methodology to measure the risk and how well the organisation has done in achieving full compliance.
- *Risk governance arrangements and frameworks*: Organisations' risk governance arrangements require risk and project owners to consider risks relating to data privacy. This means organisations have implemented clear responsibilities and a reporting structure for privacy risks and PIA and formally included privacy risks in their framework for managing organisational assets (often this means information assets) from a risk basis. Furthermore, privacy responsibilities are often shared by risk business owners and the operating management structure.

Single-risk project level

- *Procurement stage assessment*: Data protection checklist assessments, loosely based on ICO guidance, are triggered for all new procurements as part of the overall procurement risk assessment for new requisitions.
- *Information governance and risk toolkits*: Screening criteria for assessing privacy risks and the need for undertaking PIAs are formally integrated into standard information governance and risk toolkits, which organisations use to assess information risks.
- *Privacy risk integrated into project risk log and/or register*: Some organisations include privacy risk as a separate category of risk in the project risk log and register. It is then the responsibility of the project manager to maintain the risk log and to manage privacy risks in accordance with the project management approach and the corporate risk policy.
- *General risk assessment documentation and processes*: Simple and easy-to-complete data protection checklists are integrated into general risk assessment processes and documentation required for any new initiatives. Project managers responsible for the new initiative have to complete this risk assessment. Often risk management guidances, including how to assess privacy risk, are issued by organisations together

with the risk assessment documentation. This “open door” overlaps with the project management “open doors”, “regulatory gateway assessment” and “information security assessment” described in section 2.4.

- *Corporate risk management strategy and methodologies:* Clear indications on how to assess privacy risks and perform PIAs are provided to project managers in the corporate risk management strategies and methodologies.
- *Risk management training:* Privacy risks and PIA training is incorporated into the organisation’s standard risk management training.

4 FINDINGS – INTEGRATING PIAS WITH PROJECT AND RISK MANAGEMENT METHODOLOGIES

This chapter explains how PIAs are relevant to the project and risk management process. It highlights the relevance and points of congruence between PIA and project and risk management processes, as well as where they diverge. It provides a systematic analysis of how project and risk management approaches could be aligned with PIA methodologies, including that developed by the ICO and the Trilateral-developed PIA step-by-step guide,[157] which draws on the best elements of existing methodologies from Australia, Canada, Ireland, New Zealand, the UK and the US.

Our analysis results in the development of guidelines to integrate the two sides (PIA on the one side, project and risk management on the other side) as well as to improve them through a common understanding of good privacy risk management. We identify both short-term and longer-term implementation approaches. For example, we look at scenarios where a "lighter" version of PIA can be embedded, to encourage faster uptake and more immediate impact. In other cases, particularly with standards changes that require a long-term approval process, our recommendations take a more strategic view, including opportunities for the training of project management and risk management practitioners in PIA practice. As a part of this analysis, we place emphasis on evaluating methodologies preferred by ICO, and we focus on those industry sectors that are expected to have the greatest impact on privacy.

4.1 FINDINGS FROM OUR ANALYSIS OF THE PIA HANDBOOK AND OTHER PIA METHODOLOGIES

As a PIA methodology, the ICO Handbook has many good points. In revising it, or producing a third edition, the ICO should be careful not to throw the baby out with the bathwater. In view of comments made in interviews and other exchanges with organisations, our overall recommendation is that the methodology be streamlined.

The ICO Handbook suggests several deliverables in the PIA process: two in the preliminary phase (a project plan and a project background paper); three in the preparation phase (a stakeholder analysis, a consultation strategy and plan, and the establishment of a PIA consultative group); three in the consultation phase (changes to the project documents, an issues register, and a privacy design features paper); one in the documentation phase (the PIA report); and one in the review and audit phase (privacy review report). This seems too many. We suggest a single PIA report, which can be prepared and amended as necessary throughout the PIA process.

John Edwards, a PIA practitioner in New Zealand, offers some good insights into the purposes and preparation of a PIA report, which may be of value for assessors in the UK:

> If the report is to inform the project staff of privacy issues as they arise and to make recommendations which are then taken up and incorporated into the design, it will look different at the end of the project than a report prepared for a regulator or steering group. Where the assessor is working alongside the team, issues will be identified and analysed, and

[157] www.piafproject.eu

> possibly become the subject of an ameliorating recommendation. If that recommendation is picked up and incorporated into the design, the matter need not be raised in the next iteration of the report. The path of this evolving document will trace an arc from its inception to the project's implementation, and will undergo many changes over the course of the project. It will be a living document, informing decision-makers at all critical points, and at the end, will be largely spent, its purpose fulfilled.[158]

The PIA Handbook does well to emphasise that a PIA should not only consider personal data, but all four different types (or aspects) of privacy, the explanations for which are reproduced here for ease of reference:

> **Privacy of personal information** is referred to variously as "data privacy" and "information privacy". Individuals generally do not want data about themselves to be automatically available to other individuals and organisations. Even where data is possessed by another party, the individual should be able to exercise a substantial degree of control over that data and its use. The last six decades have seen the application of information technologies in many ways that have had substantial impacts on information privacy.
>
> **Privacy of the person**, sometimes referred to as "bodily privacy", is concerned with the integrity of the individual's body. At its broadest, it could be interpreted as extending to freedom from torture and right to medical treatment, but these are more commonly seen as separate human rights rather than as aspects of privacy. Issues that are more readily associated with privacy include body searches, compulsory immunisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and requirements for submission to biometric measurement.
>
> **Privacy of personal behaviour** relates to the observation of what individuals do, and includes such issues as optical surveillance and "'media privacy". It could relate to matters such as sexual preferences and habits, political or trade union activities and religious practices. But the notion of "private space" is vital to all aspects of behaviour, is relevant in "private places" such as the home and toilet cubicle, and is also relevant in "public places", where casual observation by the few people in the vicinity is very different from systematic observation, the recording or transmission of images and sounds.
>
> **Privacy of personal communications** could include various means of analysing or recording communications such as mail "covers", the use of directional microphones and "bugs" with or without recording apparatus and telephonic interception and recording. In recent years, concerns have arisen about third party access to email messages. Individuals generally desire the freedom to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations.[159]

Although other PIA guidance documents also mention these four types of privacy, the ICO Handbook provides more detail and more clarity with regard to what is at stake. We strongly support the ICO's view of privacy as being more than just data protection. We think Article 33 is seriously deficient in reducing a "privacy impact assessment" to only a "data protection impact assessment". Organisations that carry out a DPIA may be fully compliant with data protection legislation, but could still intrude dangerously into an individual's privacy. Such a risk is greatly diminished if all types of privacy are considered, as the ICO Handbook rightly argues.

---

[158] Edwards, John, "Privacy Impact Assessment in New Zealand – A Practitioner's Perspective", Chapter 8, in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, pp. 187-204 [p. 196].
[159] Ibid., p. 14.

From a comparison of the "touch points" in the PIA Handbook and the other analysed methodologies (the RFID PIA Framework, Article 33, and PIAF), we find the PIAF methodology (of which Trilateral was an author) is closest to the PIA Handbook, and is only six pages in length; annexes – for example, of questions identifying privacy risks – could admittedly make it longer. The PIAF guide takes into account the best features of existing PIA guidance documents in Australia, Canada, Hong Kong, Ireland, New Zealand, the UK and the USA. It addresses virtually all of the ICO PIA Handbook touch points and goes further than the Handbook, in saying that PIA reports should be published and subject to audit.

The PIA Handbook distinguishes between a full-scale PIA and a small-scale PIA. We think this is confusing for organisations. We do not think it is so easy to determine whether a full-scale or small-scale PIA is appropriate – despite (or perhaps even because of) the criteria in Appendix 1 of the Handbook. We suggest that, in a revised Handbook, the ICO simply say that PIAs are scalable, and that the scope, length, and intensity of the PIA will depend on how serious the privacy risks are and on the numbers of people who might be impacted.

Considering other PIA methodologies: the RFID PIA Framework was the first sector-specific PIA. The next appears to be the smart metering DPIA, a draft of which has been produced by Expert Group 2 of the Commission-initiated Smart Grid Task Force; we can envisage further sector-specific PIAs. Therefore, in a revised PIA Handbook, the ICO may wish to consider preparing a somewhat high-level, principles-based PIA methodology, perhaps with an annex of exemplary privacy risks and the questions that could be used to uncover those risks. Sectors or organisations could then use this streamlined, principles-based guide for further development of a sector- or organisation-specific PIA attuned to the specificities of their sector or organisation.

One of the major limitations of the RFID PIA Framework is that its privacy targets (a regrettable phrase in itself) are based on the principles of the Data Protection Directive (95/46/EC), whereas privacy risks (or even just data protection risks) could be wider than those addressed by the Directive. Another major limitation is its silence on the issue of stakeholder consultation or on any communication with them. While it recognises that RFID operators might need to provide a copy of their PIA reports to regulators ("competent authorities"), it does not take a proactive stance on publication of the report, even though it says that proprietary and security sensitive information could be removed from the PIA reports before providing them to regulators. The Framework is also silent on the possibility of independent third-party review of the audits of PIA reports. Perhaps the biggest question hanging over the RFID PIA Framework – especially in view of the amount of time and effort that has been consumed on this subject – is why there have been no PIA reports or, at least, none that have been brought to the attention of DPAs. If there have been no RFID PIA reports produced so far, one can assume this is because they are not mandatory. Contrast this situation with the hundreds of PIA reports produced in the UK, in Canada and in the USA, and one quickly sees the efficacy of making PIAs mandatory. Self-regulation generally does not work,[160] and perhaps the best one might say based on the evidence of the RFID Framework proceedings is that the jury is still out on co-regulation.

[160] For a scathing indictment of self-regulation, see Gellman, Robert, and Pam Dixon, *Many Failures: A Brief History of Privacy Self-Regulation in the United States*, World Privacy Forum, 14 October 2011. http://www.worldprivacyforum.org/pdf/WPFselfregulationhistory.pdf

When comparing Article 33 to the ICO PIA Handbook touch points, the shortcomings of Article 33 become clearly apparent. While Article 33 has some strong points (e.g., in making DPIAs mandatory), and while admittedly it is unfair to compare the detail contained in the 86-page Handbook with the one-page Article 33, the deficiencies of the latter are apparent all the same. The most glaring deficiency is that it is a DPIA and not PIA, i.e., its scope is much narrower than a PIA as described by the Handbook, which recognises four types of privacy. Article 33 is more focused on the report, rather than the process. It is also silent on publication of the report. It mentions specific risks without saying that these are only indicative, when the number of privacy risks could be far greater than those mentioned. It also says nothing about ensuring that DPIA report recommendations are implemented or, if not, that justification be given for not implementing them. It is also silent with regard to any changes in a project and the consequent need to revisit the DPIA.

4.2 FINDINGS FROM OUR ANALYSIS OF PUBLICLY AVAILABLE PIA REPORTS

This section highlights our findings from an analysis of PIA reports selected from the list we compiled in Annex 6. We start first with general findings, some of which have been extracted from Annex 6:

- The majority of PIA reports number fewer than 30 pages.
- The number of publicly available PIA reports is growing (slowly).
- The vast majority of publicly available PIA reports have been produced by government departments and agencies; we found only two from industry.
- Among the various stated purposes for producing PIAs are concerns about privacy impacts, and impacts on the organisation's reputation.
- Most of the PIA reports acknowledge the ICO PIA Handbook; some say they have consulted the ICO for advice on the preparation of the PIA reports.
- Some PIA reports have said that they will be updated if there are any changes in the assessed project, programme or other activity involving the processing of data. Only one such update has been found on the Internet; it is not known whether PIAs have, in fact, been updated.
- Most PIA reports appear to have been produced "in-house"; only two of the 26 publicly available PIA reports were produced by external consultants, and those two were the only discovered PIAs that emanated from the private sector. While there is nothing wrong with using external consultants to conduct the PIA – some argue that using external consultants will give the resulting PIA reports more credibility – generally organisations need to build up their own internal PIA expertise.
- Almost all of the PIA reports examined for our study show that they were undertaken before their projects were finalised, when there was still an opportunity for the PIAs to influence the design or outcome of the project; this is good practice.

Looking at specific PIAs: the PIA of the draft Communications Data bill misses several touch points. However, it is interesting nonetheless because it says that "although there are no statutory obligations on them [communications service providers] to produce PIAs they will be strongly encouraged to do so, or provide alternative equivalent assurance". This is an example, then, of the government's pushing PIAs out to the private sector. There is, as yet, no statutory obligation on companies to produce PIAs, but the pressure on them to do so is likely to grow, as this PIA from the Home Office indicates.

The PIA on smart metering, produced by the Department of Energy and Climate Change (DECC), – a better model of a thorough PIA – also pushes PIA practice onto the private sector: "This PIA should be seen as an umbrella document for the Smart Metering Implementation Programme as a whole. The Government would expect that separate PIAs on individual practices are undertaken by all data controllers, such as suppliers, network operators and third parties, involved in the processing of smart meter data, prior to the mass roll-out of smart metering." DECC clearly wants the smart metering programme to be a success so that, inter alia, the country can reap the promise of greater energy efficiencies, especially as the UK's dependence on foreign suppliers is increasing. As consumers will have the right to refuse the installation of smart meters, the government is motivated to allay any privacy concerns that consumers might have. Its strategy, to be forthright with stakeholders, including consumers, via PIAs – not only its own, but those to be produced by suppliers, network operators and other third parties – is commendable. The DECC PIA is also commendable because it engaged with a wide range of external stakeholders, undoubtedly not only because this gives its PIA more credibility, but also because these stakeholders "have directly contributed to the identification of privacy impacts". In other words, the DECC has profited from consulting external stakeholders.

One of the two PIA reports produced by the private sector – that produced by Engage Consulting – meets almost all of the PIA touch points. The other (not produced by Engage, and not included in this report) is rather poor. A good feature of the PIA on the Police National Database is that it has a foreword by the chief executive and the IMPACT Programme Director, which indicates that support and responsibility for the PIA is at the highest level. The UK Border Agency (UKBA) PIA on the Five Country Conference Protocol is interesting, not least because it is a PIA of an international agreement, the only one of its kind publicly available. It is the only one of the seven publicly available PIAs analysed in this study to include a provision for an audit of the safeguards mentioned in the Protocol. Even so, its provision is somewhat constrained, as the auditor's terms of reference would need to be agreed by all five countries.

4.3 FINDINGS FROM OUR SURVEYS

The results from the first survey, sent to 40 central government departments, local authorities and NHS trusts, show that almost two-thirds of respondents had done a PIA. Most of those carried out the PIAs in-house, using their own internal resources. This is good, since – as mentioned – organisations need to develop an in-house expertise for doing PIAs. The fact that almost half could not say how many PIAs their organisation had done might suggest that there is no central repository of PIAs, which would be unfortunate in terms of organisations' missing an opportunity to build a database, a resource that others in the organisation could use if they had to conduct a PIA.

Also of interest in this first survey was the fact that a very high percentage of organisations have a data protection officer and were aware of Article 33 of the proposed Data Protection Regulation. These findings suggest that central government departments, local authorities and NHS trusts are well aware of privacy issues, and of the importance of being careful with personal data.

For the second survey, Trilateral sent a second set of questions to the 25 respondents to our first survey. The 16 who responded to the second set stated which risk management

methodologies they were using. Although respondents were using some different methodologies, it was interesting to note that they were using one or more risk management methodologies, i.e., there is an obvious awareness within organisations of risks and the need to follow a structured approach to treat those risks. Another finding of interest is that all of the respondents consider, or are in the process of considering, privacy risks as part of their overall risk management process. This is encouraging, as this is exactly what the ICO wants to see. Also encouraging is the fact that there is close collaboration between the data protection officer and the risk manager. Such close collaboration also facilitates better integration of PIA within the risk management process.

Our third survey was much larger than the first two surveys. It comprised six questions, which were mainly variations on the first two surveys. It aimed to find out how many organisations had conducted PIAs and, of those, how many PIAs they had carried out; whether they were following particular project management and/or risk management methodologies and, if so, which ones; and whether they took account of privacy risks in their risk management process and, if so, whether the DPO and project and/or risk managers were in communication.

As Annex 2 indicated, it was not so easy to build a list of data protection officers and risk managers to whom we could send our questionnaire. If it was difficult to find such contacts within government departments and agencies, local authorities and NHS trusts, it was almost impossible for companies. The exercise in getting contact e-mail addresses showed just how great the information asymmetry is in the UK. While organisations from both the public and private sector are amassing as much personal data about citizen-consumers as they can, they hide their own most innocuous details behind an almost impregnable wall. Clearly, citizen-consumers in the UK are almost powerless compared to organisations. While the Data Protection Act 1998 might give citizen-consumers the right to access their data, this is effective negated if they cannot find out whom to ask to see such data.

By contrast, in the United States, government departments and agencies each have central registries of their PIAs, and each PIA has the name, title and telephone of the official who prepared it as well as the official who reviewed it. PIAs could become an important instrument in helping to rebalance the information asymmetry that exists between organisations and citizen-consumers – if PIAs and their publication become mandatory for the private sector where the processing of personal data may present risks to data subjects, and and if the PIA report provides the contact details of the official who is responsible for carrying out the PIA. These are several big provisos, but not necessarily insurmountable.

Of the 829 contacts to whom Trilateral sent the questionnaire directly, about 100 were companies. As mentioned, the ICO sent the questionnaire to about 1,300 contacts, almost half of whom were from the private sector. We understand that about half of those were companies. As of 25 March 2013, we had received 148 responses, with the fewest from the private sector, only 12. We suspect that the existence of FOI legislation helped to account for the much larger response rate from government departments and agencies, local authorities and NHS trusts.

The results of our third survey confirm the findings of our much smaller survey conducted in November – i.e., a high percentage (82%) of respondents follow a particular risk management methodology.

The survey responses also provide interesting insights in relation to the adoption of PIA and its integration into organisations' risk and project management processes. Based on the responses received, the majority of the surveyed organisations take into account privacy risks in the context of their overall risk and/or project management processes (83%), while 76% have established collaboration between the risk manager and data protection officer in relation to privacy risk, and 68% perform PIA.

In relation to specific sectors, central government has the highest number of organisations performing PIAs (96%), followed by NHS trusts (91%). Local authorities have the lowest number of organisations performing PIA, only 44%, with the same number not performing PIA at all.

The reasons for not performing PIAs range from the practical need of not having in place "more resources" that can take care of PIA processes within the organisation to more fundamental barriers related to the PIA processes being thought "too onerous in their current form".

Although we conclude that PIA is widely used now, perhaps a more streamlined version of the PIA Handbook would provide impetus for even greater use of PIA.

4.4 FINDINGS FROM THE CASE STUDIES

The case studies are based on interviews that we conducted with selected respondents to our questionnaire. We prepared the first set of case studies to investigate further how organisations have practically integrated privacy impact assessment into their existing project and risk management methodologies and processes, as well as to identify key lessons learned from their experience of integration and from their use of the ICO PIA Handbook The second set of case studies, those from nine to 12, specifically focus on PIA integration into policy-making together with lessons learned and use of ICO PIA Handbook in the policy-making context. For this group of case studies, we interviewed only central government departments.

Experience with PIA and the ICO Handbook

In the first case study, the company's privacy policy has been replaced by specific data privacy rules, which communicate the standards contained within the privacy policy by expressing them in the form of rules ("the rules"), all based on European data protection standards. This company uses its own bespoke project and risk management methodology. The company has integrated privacy impact assessment and risk management at the project-initiation stage via an internal, online information security assessment that addresses data protection risks. All projects have to go through a digital security check and PIA. The company's privacy team has designed a PIA to meet the company's own requirements. PIAs are sent to a central PIA repository. Integration of PIA and risk management could also be achieved at the procurement stage, before project initiation. The respondent suggested that the ICO should do some consultations with representatives of different sectors to decide what should be adapted or removed from the guidelines, and how the guidelines can be simplified, shortened and better integrated with the working of the business.

In the second case study, the company has never done any PIAs, although it is aware of PIA. It also uses its own bespoke project and risk management approach, as do many others, as we

found from the responses to the survey. It appears to be reactive, rather than proactive towards privacy concerns.

The third case study, by contrast, shows a proactive company that stresses that its privacy commitment more than complies with applicable country privacy laws: it aims to do the right thing for the millions of its customers. Strong privacy principles are at the core of the company's global privacy standards and reflect the company's commitments to safeguarding personal information in its care. The company has tailored PIA to meet its needs, but seems to have embedded privacy awareness and PIA quite well throughout its organisation. This company did not use the ICO Handbook when devising the company's initial preliminary privacy assessment and questionnaire, because the company needed a much more comprehensive and tailored PIA approach. However, the respondent also stressed that he would reconcile the company's privacy questionnaire with the ICO guidelines to be sure that the ICO recommendations are fully reflected in the company's PIA process. He appeared to be quite progressive and diligent in his concerns for ensuring adequate privacy protection, and suggested that PIAs should not only apply to "projects", but also to policies, procedures or anything involving privacy or personal data. The respondent also expressed an interest in knowing how his company benchmarks on privacy compared to others. This remark seems quite useful and interesting; i.e., the ICO could develop a set of benchmarks that companies could use to test how well they are following the ICO Handbook guidance and/or how well they integrate PIA with their project and risk management practices. Indeed, the ICO could promote the touch points developed for this study for exactly this purpose. This respondent also made the good suggestion that companies should review annually their PIA documents and processes.

The fourth case study was a of large support service company. It envisages a streamlined PIA procedure formally integrated into the company's project management process. It is designing privacy and PIA training to support the development of a privacy culture in the company. The respondent advocated a slimmed-down ICO Handbook providing more practical tools and guidance on how to assess privacy risks, since businesses do not often have the knowledge and experience required to assess privacy risks. To foster integration of privacy impact assessment with project and risk management processes, this respondent emphasised the importance of gaining buy-in from senior management and developing privacy awareness and culture within the company, sustained by effective communication and training.

The fifth case study was of an executive, non-departmental public body (NDPB) operating under the Department of Health. This NDPB has a code of practice that requires that all of the organisation's employees and suppliers take into consideration privacy impact as part of all decisions involving the use of confidential personal data, such as collecting, using and/or sharing confidential data. The organisation does not have a central PIA database or repository. As a result, the information rights manager could not estimate the number of PIAs so far undertaken. Nevertheless, the organisation has begun to design PIA considerations into its project and risk management procedures. At the start of a project, project managers need to complete a privacy assessment form for their assigned projects, which is based on 10 questions presented in the form of a risk assessment. This seems to be a good practice, and is in keeping with the approach discussed in the ICO PIA Handbook. The respondent said the Handbook should more clearly indicate the benefits of PIAs. Claiming that the Handbook gives readers the impression that the PIA process is very complex, he favoured a shorter, simplified Handbook. For improving integration of PIAs with project and risk management procedures, he recommended an extensive internal consultation involving all parts of the

organisation, which would "guarantee" buy-in. He also emphasised the importance of executive attention and of making the distinction between information security and privacy: that protecting one does not automatically ensure the other is protected.

The sixth case study concerned a local authority in London. One of the points of interest was that the council convened a half-day internal workshop of various internal stakeholders to consider the privacy impacts of new initiatives. The respondent said the council understood from the ICO Handbook that a full-scale PIA is only suitable for very large, national programmes, and that it does not apply to local government. The respondent said that more directions on how to do risk assessments within local authorities would be highly beneficial. This respondent, as did others, expressed concern about full-scale PIA taking a long time and significant resources to complete. He saw value in a "middle level" impact assessment like that used for Equality Impact Assessment (EIA). He said that local authorities should establish central PIA repositories where all the PIAs conducted by the council are stored and could be accessed. As in the case of EqIA, where councils have established such repositories, this will promote a culture of sharing and benchmarking (i.e., councils can compare how well or badly they do in relation to privacy risks and PIAs), which in turn will support learning and self-improvement.

Our seventh case study was an NHS hospital trust. The respondent claimed that the Trust has integrated privacy risks into both its existing risk and project management approaches. The integration started by developing an information governance framework where the Trust defined clear responsibilities and a reporting structure for privacy risks. The Trust also records many privacy-related risks in its own risk register, and these are routinely monitored and reported by the information-risk owner to relevant committees. For effective implementation and integration of the PIA process, the organisation needs to deliver a clear message to all project managers that the PIA process must be followed and that PIAs are an organisational requirement. The respondent also said PIA processes and tools need to be constantly adapted and monitored and this should be based on privacy outcomes.

The eighth case study was a major central government department with a small data protection team. The Department has integrated privacy risk into its annual information asset risk assessment. This annual assessment should also drive further actions on how to better integrate privacy risks and PIA processes into the organisation. However, from an operational level, the Department has not developed a formalised PIA process yet, which means that there is variation in the way in which PIA are initiated and/or undertaken. In order to achieve further integration, the respondent underlined that the cultural component, involving privacy and internal organisational culture, is important and needs to be addressed not only through privacy or PIA training. The respondent also advocated that the ICO PIA Handbook follow a basic approach, both workable and easy to implement, while addressing PIA as a business enabler.

Experience with policy-making and application of PIA

Our ninth case study was of a large central government department heading several non-departmental public bodies and executive agencies. The respondent underlined that, although the use and integration of PIA into the decision-making process is an important component for managing and addressing privacy risks early on in the implementation cycle, at present very little is done in relation to the assessment of privacy risks and application of PIA to the development of new policies and regulations. This is mainly due to a combination of factors,

ranging from the complexity of the policy-making picture and the pressure on coming out with new policies to a ministerial culture where ministers believe that they have all the answers and where privacy is not on the top of the agenda. The respondent said that a few possible actions could be taken to promote the use of PIA in the context of new policies and regulations. These actions include: clearer directions and guidelines from the ICO to the ministers underlining the importance of such assessment as well as the possible integration of PIA into regulatory impact assessment (RIA), which is an assessment tool already in use within government departments.

The 10th case study concerns a central department supported by several agencies and public bodies and responsible for a large amount of personal data. The Department has also recently endorsed an open data strategy aimed at creating a new era of accountability and openness in government by publishing accessible and reusable open data. The respondent indicated that within the Department the application of PIA to new policies and/or regulation is not formalised and tends to occur on an ad hoc basis. The respondent believed that, in order to promote the use of PIA in the context of new policies and regulations, a formalised process, requiring assessments at specific points in time during policy-making development, is not going to work. Instead, the emphasis should be on increasing awareness and understanding of privacy risks with policy-makers and providing them with training on privacy and new regulations. The ICO could also play a part by developing an easy and simplified version of PIA guidelines, specifically designed for policy-making and compressed to one page.

Our 11th case study is one of the smaller ministerial departments within the UK government. Within the Department, the application of PIA to new policies and/or regulations is not formalised and/or standardised. The respondent emphasised that doing privacy assessment for policies and regulations is not an easy task, above all in departments where the focus is on the macro (i.e., the country) rather than the micro level (i.e., citizens). This is because present PIAs, by nature, require more and specific inputs from the micro, operational level. Further barriers to the use of PIA for policy-making include decision-makers' lack of experience in privacy, lack of departmental resources, the government's recent focus on core business and lack of an internal policy that clearly indicates the need for considering privacy risk when developing new policies. The respondent pointed out that departments need clear directions on addressing privacy risks in the context of policy-making as well as workable PIA guidelines designed for policy-making. The respondent also said that the Orange Book and possibly the Green Book could provide an ideal platform for PIA guidelines designed for policy-making and consequently the ICO and the Treasury should work together to achieve this.

The 12th case study is one of the biggest ministerial departments within the UK government, dealing with a huge amount of citizens' personal data. The Department has several general policies and specific sub-policies setting up the standards that employees and contractors must follow when handling personal information. The respondent clearly indicated there is a need for consistently assessing privacy risks when developing policies and regulations. However, although the Department has developed guidelines and documentation on PIAs and has experience of doing PIA applying to policy-making, there is still a lot of variation in the way in which PIAs are used and undertaken within the organisation. The respondent pointed out several reasons why this is the case, the main being the fragmented and complex organisational structure for policy-making, lack of clarity on how to do a PIA for policy-making, overload of general PIA information and documentation for policy-makers, lack of information-sharing on performed PIAs and Ministers' culture of getting their own way.

Indeed, the respondent emphasised that a new, specific approach and process need to be designed for doing a PIA in policy-making, while public organisations should publish their performed PIAs in order to share experience and best practices. Specific recommendations for the ICO include the endorsement of a booklet style for the PIA Handbook, which should provide clear and practical guidelines on what different organisations should do for managing privacy risks as well as the ICO's firm fixing of clear and consistent breaches of the regulation.

All of the policy-making case studies strongly indicate that the use of PIA for policy-making is still a novelty, which has not been formalised or standardised within government departments. By far the most common recommendations to support and enhance the use of PIA in the context of new policies and regulations are: the development of workable guidelines specifically designed for policy-making and clear directions from the government and/or the ICO to policy-makers about the need to take privacy into consideration. Other important recommendations include increasing awareness and understanding of privacy risks by policy-makers and providing them with training on privacy and new regulations.

4.5 HORIZONTAL ANALYSIS OF THE PROJECT AND RISK METHODOLOGIES

In this section, we present a horizontal analysis of each of the 16 touch point questions across the 19 project and risk management standards and methodologies reviewed for this study. This horizontal analysis gives us a picture of the commonalities and differences between the various methodologies. It also indicates how much commonality and difference exists between the privacy impact assessment process and the project and risk management processes and, consequently, the prospects for integration.

Question 1: Does the PM/RM methodology include provisions about compliance with legislation and any relevant industry standards, code of conduct, internal policy, etc.?

Of the four project management methodologies reviewed, only one, within the European area, includes specific provisions for compliance with all the relevant legislation or industry standards applicable. It also pays special attention to the specific law regarding personal data protection. The remaining three PM methodologies have procedures that only indirectly appear to take into account legal requirements. In those cases, the requirements can only be embedded into the project specifications. Of the 15 risk management methodologies reviewed, the situation appears to be the reverse, i.e., 13 RM methodologies include clear provisions for taking into account the legal requirements. One of them focuses only on one specific privacy law, while two of them, within the European area, pay special attention to the specific law regarding personal data protection. Of the remaining two RM methodologies, one of them presents the compliance with legal or regulatory requirements as best practices which must be part of the general risk governance, while the last one only includes support for two standards.

Question 2: Is the PM/RM methodology regarded as a process or is it simply about producing a report?

Of the 19 PM and RM methodologies reviewed, most view their methodologies as a process. With regard to PM methodologies, two of them are huge and clearly produce various documents along with the project itself. This includes specifications, documentation, step

reports, etc. One of the remaining two is all about flexibility and only focuses on the project itself and its output. Four of the RM methodologies reviewed indicates that they also produce documents such as protection strategies and risk mitigation plans that must be updated on a regular basis, especially if important changes occur.

Question 3: Does the PM/RM methodology address only information privacy protection or does it address other types of privacy as well?

Of the four PM methodologies reviewed, only one, within the European area, clearly indicates that it takes into account information privacy while other types of privacy are not directly mentioned and may not be addressed at all. The remaining three PM methodologies do not address privacy at all, unless it is included in some project specifications. Concerning the RM methodologies, the situation is better. Only four of the 15 methodologies reviewed do not include any direct provision for addressing some types of privacy protection. Of those remaining, two address a wide range of risks and they include provision for taking into account privacy considerations if they are relevant for the study. Three of them specifically address information security, through the three criteria of confidentiality, integrity and confidentiality, which can also apply to personal data. Six methodologies include specific provisions for personal data protection while one of them also includes specific provisions for other types of privacy as well. Wider privacy considerations are in general out of the scope of the PM and RM methodologies reviewed in this study and information privacy is mostly the only type of privacy taken into account.

Question 4: Does the PM/RM methodology say that it should be undertaken when it is still possible to influence the development of the project?

Of the four PM methodologies reviewed, only one doesn't include any provision for this. For the three others, this is completely part of the methodology. Concerning the RM methodologies, the situation is somewhat the same. Two of the 15 methodologies reviewed only concern running systems. As such, they do not include any provision for starting at the design or development phases, for instance, though this might be doable. Nine of the 15 methodologies make clear provision for starting as early as possible in order to reduce the costs in case of any subsequent redesign. In those cases, security controls must be integrated from the outset. Between these two situations, starting as early as possible to influence the project development appears as an indirect good practice that could benefit the project. However, it's by no means mandatory.

Question 5: Does the PM/RM methodology place responsibility for its use at the senior executive level?

Of the 19 PM/RM methodologies reviewed, 15 of them provide guidance as to the placement of responsibility at varying levels of the organisation. Several of the methodologies explicitly identify the need to engage senior management in the initiation, authorisation, and validation of the project or risk framework, but for the most part, these methodologies establish the need to spread responsibility for application of project and risk management efforts across various levels of the organisation. One PM methodology indicates no participation or responsibility by senior executives, and one RM methodology calls for establishing the responsible party as an independent staff level position (IT Security Officer). The CNIL methodology is mainly targeted to the data controller, who may, in many cases be in a senior management role. In summary, the methodologies do not explicitly call for responsibility for addressing specific

risk-related issues at the senior executive level, but most provide a framework approach that supports responsibility-taking at many levels of the organisation.

Question 6: Does the PM/RM methodology call for developing a plan and terms of reference? Does it include a consultation strategy appropriate to the scale, scope and nature of the project?

There are quite mixed approaches on these issues. All the PM methodologies, not surprisingly, call for development of plans of varying scale and scope. The RM and RA methodologies focus to a much lesser degree on planning, though six of them do call for some type of plan to be developed, if only focused upon a specific area (e.g., security plan). Likewise, there is a split between PM and RM in terms of the approach to consultation with stakeholders. All the PM methodologies call for consultations of some type with stakeholders or stakeholder representatives (in the case of Agile methodologies, only "users" are consulted). The RM/RA methodologies do not tend to focus upon consultation, but instead describe "communication" with stakeholders within this context, implying a more unilateral interaction.

Question 7: Does the PM/RM methodology call for conduct of an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources)?

There is no common approach to the conduct of environmental scan amongst the methodologies reviewed. Nine of the methodologies explicitly call for conducting some type of scan for purposes of establishing context or for developing "lessons learnt" to inform the project or risk assessment. PRINCE2 explicitly calls for such activities as one of its key themes. Five of the methodologies do not have such a provision, and five others are limited in terms of the scope. For example, some of the RM/RA methodologies focus upon performing a scan of environment to identify threats. In general, there is no consistency within the methodologies, and the execution of such an environmental scan may rely in large part upon the interpretation of the methodology by, and experience of, the PM/RM practitioners engaged in the project.

Question 8: Does the PM/RM methodology include provisions for scaling its application according to the scope of the project?

For the majority of the PM/RM methodologies examined, scaling application according to the scope of the project is not a key feature, with some exceptions. Two of the four PM methodologies reviewed include tailoring as a key element or feature (PRINCE2 and HERMES). Further, for Agile-based projects, given that all work is completed in short sprints, the concept of scaling is irrelevant. PMBOK does not introduce a concept of scaling. In the RM/RA methodologies, the concept of scaling is not explicitly addressed by most of the methodologies, but the design of the methodologies enable application to different size and scale projects. There are a few specific concepts introduced, including that of the "information domain" (IT-Grundschutz) and "risk aggregration" and "impact levels" (NIST standards) that reinforce this tailoring to the context. In broad terms, scaling is addressed in the assessment of risk significance and other similar concepts featured in the RM/RA methods.

Question 9: Does the PM methodology call for consulting all relevant stakeholders, internal and external to the organisation, in order to identify and assess the project's impacts from their perspectives?

Most of the project and risk management standards and methodologies call for consulting with relevant internal and external stakeholders. Some are very explicit about doing so, such as the ISO 31000, which says that communication and consultation with external and internal stakeholders should take place during all stages of the risk management process. It also says that if risk treatment options impact stakeholders, they should be involved in the decision-making process. EBIOS makes clear provisions for "Communication and consultation on the risks" and says that involvement of all relevant stakeholders is necessary for the appropriate definition of the context and for taking their interests into consideration. NIST SP 800-30 says stakeholders are to be consulted early. Some methodologies are silent on the issue of consultation, for example, the Turnbull guidance, although the latter does distinguish between stakeholders and shareholders. Stakeholder consultation is implicit in some others. For example, IT-Grundschutz makes little or no reference to any stakeholder consultation, but does make some provision for using "external knowledge" if appropriate. Of the 19 standards and methodologies examined, 12 explicitly refer to engaging stakeholders, two imply consultation (PBBOK© and NIST 800-39) and five say no or are silent on the matter (Agile, Turnbull Guidance, IT-Grundschutz, CRAMM and NIST SP800-122).

Question 10: Does the PM methodology include provisions for putting in place measures to achieve clear communications between senior management, the project team and stakeholders?

Most (14 of 17) of the methodologies make specific provision for (clear) communications between senior management and other stakeholders. For EBIOS, communication is also considered as a key activity within the risk management process. The Turnbull guidance refers to the quality of internal and external reporting and a flow of timely, relevant and reliable information from within and outside the organisation. HERMES says communications should scale with the project size and be planned. NIST SP 800-39 and CNIL do not separately and explicitly discuss communications, but it is mentioned and is implicit in their risk management processes. NIST SP 800-30 and OCTAVE make provision for communication, but not explicitly regarding stakeholders. CRAMM and NIST SP 800-122 are silent or only make only limited provision for communication. Agile explicitly excludes senior management and other stakeholders from the communications process, and external views are brought by the user.

Question 11: Does the PM methodology call for identification of risks to individuals and to the organisation?

Most (10 of 19) of the project and risk management methodologies focus on risks to the organisation or a project, and not those affecting individuals. This includes even ISO/IEC 29100 which specifically addresses personally identifiable information, but in the context of risks to the organisation, not the individual. Some (8 of 17) project and risk management methodologies, while primarily focusing on risks to the organisation, recognise that risks may arise to individuals too. Such is the case of ISO 27005 which mentions risks to personal information, which is regarded as a primary asset of the organisation. Similarly, HERMES is mainly geared towards the risks that could endanger the project's success, but it recognises risks arising to individuals through use of their personal data. ISO 31000 is focused on risks

to the organisation, but it does say that perceptions of risk can vary due to differences in values, needs, assumptions and concerns of stakeholders. Agile does not have a risk identification process.

Question 12: Does the PM methodology include provisions for identifying protection measures and/or design solutions to avoid or to mitigate any negative impacts of the project or, when negative impacts are unavoidable, does it require justification of the business need for them?

Almost all (17 of 19) project and risk management methodologies seek to treat identifiable risks and many of those say that residual risks (those accepted by the organisation) must be justified. NIST SP 800-122 has a chapter on safeguards, but does not discuss justification. PRINCE2 recognises that aspects of a project may be objectionable to particular stakeholders, which would need to be considered in the business justification of the project. PMBOK© does not explicitly look for negative impacts of the project, and Agile does not discuss these issues at all.

Question 13: Does the PM/RM methodology include provisions for documenting the process?

Seventeen of the 19 methodologies involve documentation to varying but apparently large degrees. Most appear to be thorough and continuous throughout the process, while others indicate documentation of certain specifics (e.g., decisions and plans), and one methodology notes that documentation of a sub-process' outcome is important for another sub-process' input. One PM methodology indicates only minimal documentation, and one RM is not clear on this question but it can be supposed that documentation occurs in the PIA phase of its process. In sum, documentation is a common activity for almost all the methodologies reviewed.

Question 14: Does the PM/RM methodology include provision for making the resulting document public (whether redacted or otherwise)?

Sixteen of the 19 methodologies do not mention (or do not have) any provision for publication in the general sense, although several of them indicate some form of communication with stakeholders, or with internal personnel. One RM methodology does not publish documents except for the PIA that it includes, and another RM mentions transparency and openness with reference to personally identifiable information. Of the two (both RMs) that indicate publication, one of them says "as appropriate". In sum, publication is a rare activity for the methodologies reviewed.

Question 15: Does the PM/RM methodology call for a review if there are any changes in the project?

Seventeen of the 19 methodologies explicitly include review in their cyclical and continuous routines; updating, re-assessment, monitoring, and re-evaluation are the typical terms used. Of the two that are not so explicit, one (a PM) is very likely to include review in its cyclical process, and the other (an RM) indicates review of its risk management and risk treatment plans. In sum, review is an element in all methodologies but not so explicitly in a very small number of them.

Question 16: Does the PM/RM methodology include provisions for an audit to ensure that the organisation implements all recommendations or, if not all, that it has provided adequate justification for not implementing some recommendations?

There is considerable variation among the 19 methodologies in the requirement for auditing, and/or in the way this is interpreted. Eleven of the methodologies have either no auditing provision, or have certain provisions for review in which auditing could be envisaged as an "open door" opportunity. Of the methodologies that include auditing of compliance, this is explicit in only a very few, and in others it is carried out only in part and for a specific purpose that does not seem clearly focused on compliance. In sum, there is no clear tendency regarding auditing for implementation compliance or for justifying non-implementation, but it is perhaps the case that the methodological documents reviewed are, in many cases, in inadequate guide to what is supposed to happen. The terminology of "audit" may be too imprecise for the drawing of conclusions about this question.

Conclusions

From our review of the various project and risk methodologies, we can see some commonalities between the project and risk management processes and the PIA process. However, most of the project and risk management methodologies do not mention privacy risks or even risks to the individual. Nevertheless, to the extent that privacy risks pose risks to the organisation, the organisation should take account of such risks in their project and risk management processes, including listing such risks in the organisation's risk register. It should not be too difficult to convince organisations of the importance of taking privacy risks into account and regarding privacy risk as another type of risk (just like environmental risks or currency risks or competitive risks). Especially in industries that deal directly with the general public – for example, banking, entertainment, and retail – privacy breaches, not confined to "data breaches", can be a significant threat to the company's reputation. Based on examples of privacy breaches, it should not be too difficult to convince organisations about the need to guard against reputational risk.

Many of the risk management methodologies include provisions for taking into account information security (as distinct from privacy risks), and specifically with regard to confidentiality, integrity and availability of the information. Few go beyond this with the notable exception of ISO 29100, which specifically addresses privacy principles, IT Grundschutz and the CNIL methodology on privacy risk management. One can note that the privacy part of IT Grundschutz was written by the German DPA while CNIL which put together the privacy risk management methodology is the French DPA. Helpfully, both the privacy part of IT Grundschutz and the guides published by the CNIL include catalogues of privacy threat descriptions supplemented by the corresponding privacy controls.

Some of the project and risk management methodologies call for consulting or engaging stakeholders, especially internally, but some (e.g., ISO 31000, ISO 27005) externally as well. PIA does the same.

Some of the project and risk management methodologies (e.g., ISO 31000, ISO 27005) call for reviewing or understanding or taking into account the internal and external contexts. This is true of PIA too.

Some of the project and risk management methodologies emphasise the importance of senior management support and commitment, which is also important for successful PIAs. ICO may wish to consider some targeted campaign aimed at senior management to elicit their support and commitment to PIA and making sure their staff are aware of the importance they attach to PIA and avoiding privacy risks.

Some of the risk management methodologies call for embedding risk awareness throughout the organisation. Some call for training staff and raising their awareness, which is also essential to PIAs.

Of the four PM methodologies reviewed, only one (Hermes) includes clear provisions for being compliant with a personal data protection law. By contrast, many of the risk methodologies say that organisations should comply with regulations; PIA does that, although it should also focus on risks that may not be covered by simple compliance with legislation. There is little emphasis in the project management methodologies on compliance.

There is an important difference in the focus of project and risk management methodologies, respectively. Put simply, *project* management is about managing projects. To the extent that good project management should be aware of risks and not let them impede the critical path, there are opportunities for bringing PIA into the project management process. However, PIA is about identifying and resolving privacy risks, so their natural affinity is much closer to – indeed congruent or aligned with – *risk* management. Consequently, if the ICO were going to expend resources in attempting to improve the integration of PIA with project and risk management practice, there will probably be less resistance from organisations that use *risk* management methodologies.

Almost all of the methodologies are silent on the issue of publishing the project or risk management report, although some do attach importance to documenting the process. Similarly, most are silent on the issue of independent, third-party review or audit to the project or risk management reports. There is, however, a requirement for companies listed on the London Stock Exchange to include information in their annual reports about the risks facing the company and how the company is addressing those risks.

From a strategic and/or tactical point of view, ICO should expend effort in attempting to insert PIA into the most popular project and risk management methodologies. As these methodologies are periodically revised and updated, there should be opportunities for doing this. It would mean that the ICO should take a more active (but focused) role in the relevant bodies for where these methodologies are considered, e.g., in the BSI panel that provides inputs into the ISO.

4.6 SUMMARY OF "TOUCH POINTS" AND "OPEN DOORS"

In this section, we review our conclusions and recommendations at the end of each project and risk management methodology, to see if we can identify some commonalities or spot some differences with regard to the "touch points"– i.e., points of commonality between the PIA process and the project/risk management methodologies – and the "open doors" – i.e., where a PIA could interface with the project or risk management methodology or when in the project or risk management process a PIA could be conducted in whole or in part.

Project management methodologies

The dominant project management methodologies (PMBOK and PRINCE2) were examined, and though they differ significantly, they share a structured, process-driven approach to managing projects towards specific, well-defined business objectives. This structured approach provides a good basis for integration of PIAs. In each case, the methodology does not include any specific focus upon the core issues of privacy and data protection, but rather, provides a framework within which these issues can be addressed.

With a highly structured framework, **PMBOK** offers the opportunity to examine privacy and data protection issues alongside other regulatory and legislative factors when developing the project charter and scope, as well as within the context of ongoing change control. This enables privacy to be addressed both at the beginning point of the project where design and direction can be influenced, and as part of an ongoing process to ensure continued compliance and responsiveness to recommendations.

For **PRINCE2**, which includes tailoring for scale and scope as a key element of the framework, there are numerous points in the methodology where PIA may be effectively introduced. In particular, privacy and data protection should be included as risks to be evaluated, with PIA introduced in the **M_o_R** (Management of Risk) companion methodology as a technique for evaluating and controlling these risks. Privacy and data protection standards should be established on an overarching basis within the context of the Business Case theme of PRINCE2.

Technology development management methodologies

We examined two technology development management methodologies, Agile and HERMES. In point of fact, **Agile** is not a single methodology, but rather a number of methodologies that share a set of common practices all geared towards high levels of user involvement, continual examination and validation of product, and frequent releases of deployable product. Of these methodologies, **SCRUM** is the most widely applied. The Agile methodologies do not have a specific concept for embedding privacy and data protection principles, but there are two potential approaches for introducing these principles, either through the development of a user story into the product backlog to be developed, or as a standard of "doneness".

As with Agile methodologies, **HERMES** lacks provisions for broad privacy protection. However, the tailoring feature of HERMES provides the opportunity to include project-specific requirements and objectives; in this case, privacy and data protection could be introduced through the requirement for a broad privacy analysis. The quality management sub-model enables verification and audits to be performed to ensure recommendations emerging from this privacy analysis have been integrated into the project after completion of the analysis.

Risk management

Of the risk management methodologies we examined, **ISO 31000** appears to be the most prevalent risk management methodology. It shares some "touch points" with PIA, but because it is a generic risk management methodology, it does not address some PIA issues – for example, it does not use the word "privacy", not is there any provision that might suggest

recognition of data protection risks. However, communication and consultation with stakeholders are integral to the risk management process, hence, there are some "open doors" in the process where a PIA could be conducted. There is nothing in the standard that would be at odds with a PIA.

From a review of our 16 touch points, we can see some comparability between PIA and the **Turnbull guidance**. There is nothing in the Turnbull guidance that would act as a barrier to including a PIA in a listed company's risk management process.

Although the **Orange Book** does not focus on risks to individuals, many of the points in its risk-management methodology seem compatible with PIA, and the way it addresses risk through an analysis of preventive and corrective controls could also provide a gateway for considering privacy impact as part of a mitigating strategy. So, too, could the Orange Book's concern with stakeholder expectations. Its discussion of potential risks brought about by new projects could also provide an "open door" if such projects involved new IT projects and systems, for which the need for PIA could be identified within a privacy risk management routine.

The **ENISA** risk management methodology meets many of the PIA "touch points". It offers several "open doors" (or interfaces) for integration of its risk management methodology with other corporate operational processes. Also of interest is ENISA's distinction between existing and emerging risks, and its approach to each. It manages existing risks using a somewhat tried and tested (but traditional) risk management approach, whereas it uses relatively elaborate scenarios to explore emerging risks.

Information security

With regard to the four information security risk management methodologies that we reviewed, **ISO 27005** has many "touch points" in common with the PIA Handbook. One can see several "open doors" too: it could be done during the environmental scan (context establishment) phase; it could be done as part of the risk identification process (common to both ISO 27005 and PIA); it could be done during the process of identifying controls (counter-measures) against the risks; and it could also be done in preparing the risk treatment plan. The most appropriate part would be in identifying risks and, subsequently, controls.

IT-Grundschutz identifies typical threats regarding compliance with the law as well as their corresponding safeguards, which helps to align it with the PIA process. However, regarding interactions between this methodology and PIA, IT-Grundschutz lacks some components, e.g., consultation with stakeholders, environmental scans, and broader privacy consideration.

NIST 800-39 is an elaborate document that, with NIST SP 800-30, gives a highly detailed guide to risk management in all its stages, procedures, structures and thought-processes. There may be "touch points", "open doors", and other affordances in NIST 800-39 and in the PIA Handbook that could be worth developing. Although hardly any mention is made of privacy, the specific focus of 800-39 on security risk should not rule this out, especially if 800-30 is implemented in conjunction with it and if the latter can be oriented more firmly towards PIA. If PIA can be inserted into the security concerns of 800-39, PIA responsibility could be grafted onto the role of "risk executive (function)" in the governance and decision-making structure for risk management.

For purposes of identifying a window for inclusion of PIAs within the **COBIT** framework, many of the key elements of PIA are implicitly included in the framework, which calls for adherence with external compliance and regulatory factors.

5 RECOMMENDATIONS

This final chapter provides recommendations on how the findings of this report can be incorporated into guidance produced by the ICO and other bodies, and on the practical steps the ICO can take to promote a better fit between PIA and project and risk management standards and methodologies such as those described in this report. A set of recommendations for organisations is also provided, and play an important part in the promotion of PIA as a crucial process in the public and private sectors. It is not easy to introduce new standards and/or methods into multi-stakeholder organisations, and timelines for acceptance and integration into certification and accreditation schemes are lengthy. For this reason, these recommendations accommodate both the rigorous requirements for consideration in formal risk and project management methodologies, and the more practical matters of short-range implementation by practitioners. Each recommendation draws upon the information and analysis presented in earlier chapters as well as in the annexes. Below each recommendation are brief explanatory notes, some of which recapitulate relevant conclusions and recommendations made in Chapter 4's analysis of methodologies.

5.1 RECOMMENDATIONS FOR THE ICO

1. *We recommend that the ICO develop measures aimed at promoting a closer fit between PIA and risk- and project-management methodologies through direct contact with leading industry, trade, and other organisations in both the public and private sectors.*

The survey responses shown in this report are encouraging, and it is likely that such promotion would be directed at a relatively well-informed and responsive constituency. Specific operational measures are indicated elsewhere in these recommendations, but the ICO could play an important part by encouraging their implementation. Proactive ICO consultation and workshops with industry sectors would be helpful in this, perhaps as a defined project in the near future, involving ICO, relevant organisational managers, and external advisers. Where relevant, lessons might be learned from organisations (e.g., local authorities) that have integrated Equality Impact Assessment into their managerial and governance processes.

2. *We recommend that, in revising its PIA Handbook, the ICO make the third edition much shorter, more streamlined, and more tailored to different organisational needs. It should be principles-based and focused on the PIA process. The ICO should undertake a consultation on a draft of a revised guidance document.*

All of the case-study respondents called for a shorter, more streamlined methodology. A new format for the Handbook, based much more on booklet style, would also significantly improve the Handbook by offering an easy way to select and find the right information for different readers. A new edition could be guided in length and style by the "Step by Step Guide to PIA" that was produced for the PIAF project. It would be useful to have an annex identifying various types of privacy risk and a set of questions designed to uncover specific risks. There are early signs of a trend toward sector-specific PIA frameworks or templates (e.g., RFID, smart grid), but organisations are also tailoring PIAs to their specific needs. The revised Handbook should encourage this trend by showing examples. These sectoral and organisational approaches point to the importance of the ICO's promoting a set of PIA principles in any revised guidance. In addition, the relevance of PIA to changes in

organisations' personal-data processing should be highlighted, even where new projects or technologies are not clearly involved in these changes.

3. *We recommend that the ICO's guidance on PIA emphasise the benefits to business and public-sector organisations in terms of public trust and confidence, and in terms of the improvement of internal privacy risk-management procedures and organisational structures.*

It is important that PIA – and for information privacy protection generally – should not be seen as a "barrier" or a bureaucratic nuisance and expense, but as an asset in information management. Some organisations already realise this but the message is not generally appreciated, and the link between PIA and these benefits needs to be clarified and demonstrated through guidance and advice materials. The focus should be on emphasising the business value of doing PIA (which could be more than just trust and confidence) and how PIA can work as a business enabler.

4. *We recommend that ICO guidance help organisations to understand and evaluate privacy risk, whether or not they can integrate PIA into their risk-management routines and methodologies.*

Risk and its assessment are at the heart of PIA, but there are many issues involved in estimating levels or risk, risk probabilities, risk severity, the social distribution of risk, and other topics. Only some of these are handled in generic risk-management methodologies in ways that help in the case of privacy risk, and guidance is likely to be needed so that PIA is not used as a blunt tool or inappropriately in cases where it is possible to construe everything as "a risk" in one sense or another. Guidance of this kind may have the beneficial effect of helping organisations to decide on the kind or level of PIA they ought to perform.

5. *We recommend that the ICO develop a set of benchmarks that organisations could use to test how well they are following the ICO PIA guidance and/or how well they integrate PIA with their project- and risk-management practices, especially where there are "touch points".*

The analysis of PIA reports shows significant variation in their quality and adherence to the PIA Handbook touch points. The ICO should take steps to ensure good quality and adherence by developing relatively simple benchmarks against which organisations could evaluate their own PIA performance against the Handbook or guidance, and by producing specific guidance for organisations in integrating PIA with project- and risk-management methodologies. The 16 touch points used in this report could form the basis of the benchmarks.

6. We recommend that the ICO strongly urge PIA-performing organisations to report on how their PIAs have been implemented in subsequent practice, and to review the situation periodically.

Most PIAs reviewed in this report seem to lack any information on whether the government departments, agencies or others in question have accepted the PIA recommendations (the Scottish government's e-Care PIA is an exception.), whereas, in Australia, for example, it is often the case that the organisation makes a response saying which recommendations it has accepted and the reasons for rejecting any. In the UK, this would give greater assurance to citizens and consumers that not only has the organisation performed a PIA, but also that it has been more than a perfunctory exercise, that the organisation has considered seriously the PIA report's recommendations, and that it has explained how they have been implemented.

7. *We recommend that the ICO promote to organisations the benefits of establishing repositories or registries of PIAs. We recommend that the ICO compile a registry of publicly available PIA reports, or at least a bibliography of such reports.*

Public organisations should publish their performed PIAs in order to share experience and best practices. Organisations can employ a registry as part of its "corporate memory" (i.e., what happened in a particular case), and as a way to learn lessons, to foster good practice, to promote a culture of benchmarking, and to demonstrate to citizens and consumers that the organisation takes privacy seriously. Where an organisation is composed of disparate braches that follow different trajectories in undertaking PIA, a repository can help in intra-organisational learning and the promotion of good PIA practice. US government departments and agencies have created such registries. The UK government has done something similar with a repository of Equality Impact Assessments and Regulatory Impact Assessments. Annex 3 to the present report could be the starting point for a registry or bibliography. Moreover, local authorities need to establish central PIA repositories where all the PIAs conducted by the council are stored and can be accessed. As in the case of equality impact assessment, where councils have established these repositories, this will promote a culture of sharing and benchmarking (i.e., councils can compare how well or badly they do in relation to privacy risks and PIAs), which in turn will support learning and self-improvement.

8. *We recommend that the ICO take advantage of the current work within ISO to develop a PIA standard, and the BSI's technical panel's contribution to it.*

We see a good, strategic opportunity to ensure a closer fit between PIA and risk management through the work being done in the ISO to develop a PIA standard. The UK BSI technical panel is providing inputs to the ISO, and the ICO's participation directly or as an observer would be desirable. ISO standards are revised from time to time. If this happens with ISO 31000, the ICO could urge the BSI (as an ISO member) to make more explicit potential risks to privacy and data protection. The existence of ISO 29100, which addresses privacy principles, is helpful in this regard, as are the efforts of other DPAs (e.g., CNIL and Ontario) to encourage privacy risk management and "privacy by design".

9. *We recommend that the ICO audit the PIA process and PIA reports in at least a sample of government departments and agencies*.

The Office of the Privacy Commissioner of Canada has undertaken such audits; based on its findings and recommendations, the audit process itself was instrumental in raising the quality of the PIA process and reports. Similarly positive results could be obtained in the UK.

10. *We recommend that privacy risk be taken into explicit account in the Combined Code for companies listed on the London Stock Exchange.*

The ICO should brief the Financial Reporting Council (FRC) on the efficacy of PIA. The ICO could ascertain from the FRC whether there is a possibility to strengthen the Turnbull guidance and/or the UK Corporate Governance Code with more specific provisions regarding privacy risks, and to encourage companies to undertake a PIA in order to identify and respond to privacy risks. ICO could cite the PIA performed by the Department of Energy and Climate Change (DECC) as an example of a relatively good PIA, and note that the Energy Networks

Association undertook its PIA in order to foster transparency and consumers' trust. Similarly, the ICO could point to other companies that undertake PIAs (such as Vodafone, Siemens and Nokia) and the importance these companies attach to their reputation as a core corporate asset.

11. *We recommend that privacy risk be inserted into government guidance such as the Treasury Orange Book and the Green Book on appraisal and evaluation in central government.*

The *Orange Book* and the *Green Book* – both directed at government departments – are a possible place for including in the policy process focused guidelines on privacy risks. Indeed, there is already recognition that the Orange Book should include some sections on privacy risks and PIAs, and the Treasury may soon address this. Although the *Orange Book* does not engage with privacy or with risk to individuals, its risk management cycle has "open doors": its discussion of potential risks posed by new projects and its concern for stakeholder expectations provide opportunities for the ICO to promote PIA in any revision of the *Orange Book*. The *Green Book* similarly is not concerned with privacy impact, but the latter appears also to afford "open doors' in its approach to risk assessment and management.

12. *We recommend that, at senior ministerial and official levels in government departments, and among special advisers, the ICO engage in dialogue to underline the importance of privacy and PIA while developing new policy and regulations and in the communication plans accompanying new policies.*

Cultural barriers to an appreciation of the importance of privacy protection within departments need to be addressed, so that PIA awareness can permeate the organisation. There need not be a formalised PIA process for policy-making, requiring assessments at specific points in time during the policy-making development, which would create unnecessary paper trails for policy-makers. Instead, the emphasis should be on increasing awareness and understanding of privacy risks with policy-makers and providing them with practical training on privacy and new regulations so that they can recognise when they need to involve the department's data protection personnel. Departmental internal policies should clearly state that there is a need to take privacy risks in consideration during the regulatory process, while providing tools and guidelines on how to do it. However, it may be that the PIA Handbook as such, and as a whole, is not well suited to the macro level of policy making, because it is focused on handling data and personal information. Ways of developing a new, specific approach for doing a PIA early in the policy-making process should be explored between the ICO and central departments. The ICO and the Treasury could also work together to develop a policy-making-based PIA approach and practical guidelines. In addition, senior departmental policy-makers could explore the relative advantages of either integrating PIA within the existing regulatory impact assessment (RIA) process – an assessment tool already in use within government departments that aims to help decision-makers understand the potential positive and negative effect of contemplated policy initiatives – or of keeping it as a separate instrument.

13. *We recommend that the ICO encourage the Treasury to adopt a rule that PIAs must accompany any budgetary submissions for new policies, programmes and projects.*

This is the case in Canada, and we believe it can play a useful part in UK government.

14. *We recommend that the ICO encourage ENISA to support the ICO initiatives with regard to insert provisions relating to PIA in risk management standards as well as within ENISA's own approach to risk assessment.*

ENISA has promoted good risk assessment and risk management practices, including privacy risks, and ENISA is well aware of PIA issues. It contributed to the assessment of the RFID PIA Framework proposed by industry before the Article 29 Working Party endorsed the Framework. It has had many expert groups considering emerging and future risks. ENISA plays an important role throughout Europe regarding information and communications risk management. Hence, it is in a position to influence the adoption of PIA by industry, government and others in the UK (and elsewhere in the EU). The ICO could encourage ENISA to make more specific references to the utility of PIA in its guidance documents.

15. *We recommend that the ICO accelerate the development of privacy awareness through direct outreach to organisations responsible for the training and certification of project managers and risk managers.*

These organisations would include, for example, PMI (PMBOK), ISACA (COBIT), APMG (PRINCE2), ICAgile (or others that certify Agile practitioners). Because the process to implement broader PIA uptake through standards board and organisations can be anticipated as lengthy, it would be useful simultaneously to focus efforts to increase privacy awareness through professional development/training organisations. Those individuals working across a range of industries and sectors can develop their skills to keep pace with the evolution of privacy regulations and their practical application to effective project and risk management. While there is a greater awareness and knowledge of privacy impacts within public-sector projects and organisations at present, with changing regulations, there will be a growing need for professionals who can apply this knowledge to ensure privacy and data protection are effectively addressed in new systems as they are developed, regardless of industry or sector. Moreover, we believe that project and risk management practitioners can increase their own value to organisations by increasing privacy awareness amongst team members on a project basis, or during risk management planning and monitoring activities.

5.2 RECOMMENDATIONS FOR COMPANIES AND OTHER ORGANISATIONS

This set of recommendations can only indirectly be enjoined on organisations, to which this report is not addressed, and are therefore more likely to be considered if they are mediated by strong ICO guidance and promotion. These recommendations are based on the findings of the survey, interviews, and other findings in the report. Some of these recommendations focus on how organisations could operationally better integrate PIA into existing project management and risk management approaches. Although there is no single path for integration, but instead different options are open to different organisations allowing alignment with specific organisational requirements, our review of the "touch points" and "open doors", as well as findings from the interviews and survey, indicate some useful best practices for achieving operational excellence in PIA integration.

16. *We recommend that, to help embed PIA and to integrate it better with project and risk management practices, a requirement to conduct a PIA be included in business cases, at the inception of projects, and in procurement procedures. Organisations should require project*

managers to answer a simple PIA questionnaire at the beginning of a project or initiative to determine the specific kind of PIA that should be undertaken.

Organisations should consider privacy risk and PIA not only for projects but for any business activities and organisational changes that could have an impact on privacy (e.g., internal policy, such as Human Resources regulation, or changes in organisational structure and processes). Furthermore, a simple and easy initial PIA screening should be integrated into any type of project documentation in use, either on-line or paper based (e.g. project initiation document, regulatory screening, environmental scan, security assessment, etc.), that project managers are required to complete at the inception phase of a project.

17. *We recommend that senior management take privacy impacts into consideration as part of all decisions involving the collection, use and/or sharing of personal data.*

This, and certainly the undertaking of PIA, will require consultation with the organisation's stakeholders. In consulting stakeholders, organizations should be proactive and seek them out. Simply posting notice of a consultation on the organisation's website is not enough to engage stakeholders.

18. *We recommend that companies and other organisations review annually their PIA documents and processes, and should consider the revision or updating of their processes as a normal part of corporate performance management.*

The interviews and responses in this report show that it has emerged as good practice that some organisations that have achieved a good level of maturity in relation to privacy and PIA, while leading the way in the use and integration of PIA into existing processes, have implemented these measures as part of their internal monitoring and checking procedures. The PIA annual review is often done in parallel with the review of overall risk management procedures. Senior managers discuss and assess how well the organisation has performed in relation to its privacy objectives, and assess whether the implemented PIA processes and tools have been adequate. This review provides a systematic and periodic process for assessing the organisation's privacy performance in relation to certain pre-established criteria and organisational objectives, while identifying needs for further enhancement and next steps.

19. *We recommend that companies and other organisations embed privacy awareness and develop a privacy culture, and should provide training to staff in order to develop such a culture. High priority should be given to developing ways of incorporating an enhanced PIA/risk assessment approach into training materials where information-processing activities pose risks to privacy and other values.*

While our prior recommendations include ways to move from the top down in enhancing standards for project and risk management, these approaches will likely take time to be integrated and disseminated. Therefore, we believe that organisations will need to take a proactive stance to prepare their organisations for privacy-aware software development approaches. In particular, in the case of Agile development environments, developers on the front line need to address privacy within the core definition of doneness within each iteration of developed product.

20. *We recommend that companies and other organisations include contact details on their PIA cover sheets identifying those who prepared the PIA and how they can be contacted. The*

PIA should promote the provision of a contact person as "best practice". Such practice needs to be made mandatory certainly within any government organisation and any organisation doing business with the government. Such practice should also be promoted within standards organisations.

It remains a discouraging fact that it is difficult for individuals to ascertain who is responsible for information privacy and data protection matters in organisations. Many organisations do not publicise contact names and e-mail addresses so that people can pursue legitimate requests for subject access, or indeed for more general inquiries relating to PIA and other relevant matters. If PIA is made mandatory, it should include contact details on the cover sheet, as is done in the US, regarding who prepared the PIA and how to get in touch with that person. The ICO should promote the provision of a contact person as best practice, although we are sure that "promotion of best practice" will have only minimal impact. Such practice needs to be made mandatory certainly within any government organisation and any organisation doing business with the government. Such practice should also be promoted within standards organisations.

21. *We recommend that public-sector organisations insert strong requirements in their procurement processes so that those seeking contracts to supply new information systems with potential risk to privacy demonstrate their use of an integrative approach to PIA, risk management and project management.*

These organisations could thus exert leverage upon contractors whose goods and services may pose threats to the privacy of those with whom an organisation deals when it uses information systems. Making such a demonstration an eligibility requirement for tendering could have a useful effect, as well as simplifying the subsequent risk assessment work that the organisation itself performs when implementing information systems.

22. *We recommend that companies and other organisations include privacy in their governance framework and processes in order to define clear responsibilities and a reporting structure for privacy risks.*

From the interviews, this appears to be a necessary step in order for organisations to start formalising PIA processes internally and integrating PIA into their risk and project management operational processes. If organisations do not have a senior manager clearly responsible for the final outcome within the organisation (i.e., management of the privacy risk), the final outcome will not happen. This does not necessarily mean that organisations need to develop a new governance framework: they just need to clearly allocate privacy responsibility within their existing framework.

23. *We recommend that companies and other organisations include a PIA task, similar to a work-package or a sub-work-package, in their project plan structures in order to embed PIA better within project management practices, and that project managers monitor and implement this new privacy task, based on the identified privacy requirements, as is done in the case of other project tasks.*

The findings from our interviews and survey have indicated that a few organisations, leading on PIA integration, have adopted this approach as best practice; this is also consistent with our review of key "touch points". This route has been formally taken by HERMES, for example. The addition of a specific task for privacy in the project plan will enable a clear

identification of the necessary resources and activities required to do the work, while monitoring privacy progresses and results during the lifetime of the project.

24. *We recommend that, to foster internal buy-in for any newly adopted processes and procedures, companies and other organisations undertake extensive internal consultation with all parts of the organisation involved in risk management and project management, when thinking of integrating PIA into existing organisational processes.*

Most new processes and plans fail if there is no buy-in and real engagement across the different levels of the organisation. As the survey findings underline, this is an important challenge in relation to PIA. Since a solid PIA process involves several departments, it is important to get involvement and engagement right from the beginning by making sure that those who implement the new procedures and processes have a say in how these processes will work in practice.

25. *We recommend that companies and other organisations include identified privacy risks in their corporate risk register, and that they update their register when new or specific types of privacy risk are identified by implementation teams.*

Interviews and survey findings suggest that this is a useful good practice. The inclusion of identified privacy risks in the corporate register allows organisations to build an internal catalogue of specific privacy risks to use for internal reference when assessing privacy risks for existing and new initiatives. When developing this list, it is also important that organisations view risks not only exclusively from their own internal perspective (i.e., risk of reputational damage) but also include the perspective of the citizen or customer (i.e., risk of distress and financial loss).

26. *We recommend that companies and other organisations develop practical and easy guidance on the techniques for assessing privacy risks and actions to mitigate them.*

Organisations could use ENISA, ISO 27005, CNIL, NIST 800-122 or EBIOS methodology to develop a practical, internal guide on how to assess privacy risks. The guide will improve standardisation and consistency on how to assess privacy risks within the organisation, while supporting project managers in doing their privacy assessment. Organisations should also think of involving external stakeholders, such as end-users and civil society, as part of their approach to privacy risk assessment. External stakeholders could bring valuable, external insights and a customer or citizen point of view, which are necessary for the effective assessment of privacy risks.

6 ANNEX 1 – PIA PRACTICES

In this annex, we summarise the key points from the ICO's PIA Handbook and conclude that first section with a table listing various "touch points", as we have termed them. We have used this table of touch points as a means of analysing other PIA methodologies, several publicly available PIA reports as well as the various project and risk methodologies. In analysing these other reports and methodologies, we wanted to see whether they had some touch points in common with those we have identified from the ICO PIA Handbook. We assume that the prospects for better integration of PIA with project and risk methodologies will be greater if they share some touch points in common.

Following our review of the PIA Handbook, we have analysed three other PIA frameworks, namely, the RFID Framework which was endorsed by the Article 29 Data Protection Working Party in February 2011, Article 33 of the European Commission's proposed Data Protection Regulation, which would make PIA mandatory where organisations processing personal data present risks to data subjects, and the PIAF methodology which emerged from a project funded by the EC's Directorate General Justice and in which Trilateral was a partner.

We then review several publicly available PIA reports to see how well they track the guidance provide by the PIA Handbook.

6.1 KEY FEATURES AND RECOMMENDATIONS FROM THE ICO PIA HANDBOOK

The Information Commissioner's Office (ICO) *Privacy Impact Assessment Handbook*, revised in 2009,[161] regards PIA as "a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions."

As already mentioned above, the Cabinet Office, in its Data Handling Review, called for all central government departments to "introduce Privacy Impact Assessments, which ensure that privacy issues are factored into plans from the start".[162] It accepted the value of PIA reports and stressed that they will be used and monitored in all departments from July 2008 onwards. PIAs have thus become a "mandatory minimum measure".[163]

The 86-page ICO Handbook is divided into two main parts: Part I (Chapters I and II) provides background information on the PIA process and privacy. Part II (Chapters III – VII) is a practical "how to" guide on the PIA process. The Handbook also has four appendices: on PIA screening questions, a data protection compliance checklist template, Privacy and Electronic Communications Regulations (PECR) compliance checklist and privacy strategies.

---

[161] ICO, *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, UK, Version 2.0, June 2009. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html, http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

[162] Cabinet Office, Data Handling Procedures in Government: Final Report, June 2008, p. 18. http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf

[163] See Cabinet Office, Cross Government Actions: Mandatory Minimum Measures, 2008, Section I, 4.4: All departments must "conduct privacy impact assessments so that they can be considered as part of the information risk aspects of Gateway Reviews". http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf

The Handbook says that, because organisations vary greatly in size, the extent to which their activities intrude on privacy, and their experience in dealing with privacy issues makes it difficult to write a "one size fits all" guide.

The ICO envisages a PIA as a process, separate from compliance checking or data protection audit processes[164] that should be undertaken when it can "genuinely affect the development of a project".[165] The Handbook distinguishes a PIA from a privacy or data protection audit. An audit is conducted post implementation of a project, a PIA prior to it. An audit confirms compliance privacy undertakings and/or privacy law and highlights problems that need addressing while a PIA intends to prevent problems.

According to the Handbook, a PIA is necessary for the following reasons: to identify and manage risks; to avoid unnecessary costs through privacy sensitivity; to avoid inadequate solutions to privacy risks; to avoid loss of trust and reputation; to inform the organisation's communication strategy and to meet or exceed legal requirements.

A PIA "also helps mitigate the risk of retrospective imposition of regulatory conditions as a response to public concerns about the project, with inevitable additional and unbudgeted costs or even the entire project being put at risk of being in non-compliance with the new laws. A PIA provides an organisation with an opportunity to obtain a commitment from stakeholder representatives and advocates to support the project from an early stage, in order to avoid the emergence of opposition at a late and expensive stage in the design process."

Regarding identifying and managing risks, the Handbook says that "At senior levels of organisations, a PIA is part of good governance and good business practice. A PIA is a means of addressing project risk as part of overall project management. Risk management has considerably broader scope than privacy alone, so organisations may find it appropriate to plan a PIA within the context of risk management."

The Handbook points out that "Designing in privacy solutions can make a project more resistant to a failure around individual privacy and better able to recover if a failure does occur. Bolt-on solutions devised only after a project is up and running can often be a sticking plaster on an open wound, providing neither the same level of protection for the individual nor the confidence for the organisation that privacy risks have been identified and adequately addressed."

The Handbook says that a PIA enables an organisation to understand the perspectives of other stakeholders and make the aims of the project better understood. It also provides stakeholders the opportunity to have their perspectives reflected in the project design.

The Handbook repeatedly stresses the importance of consulting stakeholders: "By actively seeking out and engaging the concerns of stakeholders, even those who are expected to oppose a particular project, the project manager can discover the reasoning behind their position and identify where further information needs to be provided and pre-empt any possible misinformation campaigns by opponents of the project."

[164] ICO Handbook 2009, Part I, Chapter I.

[165] Ibid. The Handbook uses the term "project" as a catchall; it can refer to "a system, database, program, application, service or a scheme, or an enhancement to any of the above, or an initiative, proposal or a review, or even draft legislation".

Elsewhere, the Handbook points out that during the PIA, stakeholders might raise concerns that the organisation has not considered or might put much greater weight on concerns that it had identified but dismissed. It also says that if the analysis is undertaken solely from the viewpoint of the organisation itself, it is likely that risks will be overlooked.

The Handbook stresses that measures are needed to achieve clear communications between senior management, the project team and representatives of, and advocates for, the various stakeholders.

The Data Protection Act already stipulates eight data protection **principles**, but these only address certain aspects of privacy. There are a range of other pieces of legislation which have an impact on privacy and either empower or prohibit certain acts which may intrude upon the privacy of the individual.[166]

The Handbook identifies four **types of privacy** to be considered by a PIA:

- privacy of personal information;
- privacy of the person;
- privacy of personal behaviour; and
- privacy of personal communications.[167]

Additionally, the Handbook highlights the results of an effective PIA:[168]

- the identification of the project's privacy impacts;
- an appreciation of those impacts from the perspectives of all stakeholders;
- an understanding of the acceptability of the project and its features by the organisations and people who will be affected by it;
- the identification and assessment of less privacy-invasive alternatives;
- an identification of ways in which negative impacts on privacy can be avoided;
- an identification of ways to lessen negative impacts on privacy;
- where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them; and
- documentation and publication of the outcomes.

The Handbook says that PIA should be conducted early in the project development so that risks and problems can be identified and managed efficiently. For projects already in existence, the Handbook says that the time to act is the present. The ICO conceives of a PIA as a "cyclical process linked to the project's own life-cycle; and re-visited in each new project phase".[169]

Management of the PIA

[166] ICO, *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, UK, Version 2.0, June 2009, p. 6. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html
[167] ICO, PIA Handbook, p. 14.
[168] Ibid.
[169] ICO Handbook, Part I, Chapter I.

The Handbook places responsibility for managing a PIA at the senior executive level (preferably someone with lead responsibility for risk management, audit or compliance).

Furthermore, the Handbook advises that the terms of reference for the PIA should include the following:[170]

- the functions to be performed;
- the deliverables;
- the desired outcomes;
- the scope of the assessment; and
- the roles and responsibilities of the various parties involved in the PIA.

Role of the Information Commissioner

The ICO does not play a formal role in conducting, approving or signing off PIA reports. It does, however, play an informative and consultative role in supporting organisations in the conduct of PIAs.

The PIA process

The ICO identifies five phases in a PIA: preliminary, preparation, consultation and analysis, documentation, and review and audit. These phases occur in both full-scale and small-scale PIAs, though they differ in scope.[171]

1. Preliminary

This phase focuses on establishing a firm basis for the "effective and efficient" conduct of the PIA. The Handbook suggests two deliverables for this phase – a project plan and a project background paper. Tasks suggested for this phase include: reviewing outcomes and documents from the initial assessment; developing the project outline;[172] ensuring appropriateness of terms of reference, scope and PIA resources; preliminary discussions with relevant organisations and stakeholder groups; preliminary analysis of privacy issues; and preparation of the project background paper.

2. Preparation

In this stage, arrangements are made in anticipation of the critical consultation and analysis phase. The ICO Handbook suggests the following deliverables for this stage: a stakeholder analysis, a consultation strategy and plan, and establishment of a PIA consultative group (PCG). It says that any consultation should be appropriate to the scale, scope and nature of the project for which a PIA is being completed. In order to make the maximum contribution to risk management in return for the smallest cost, consultation needs to commence early and continue throughout the project life-cycle. The assessor needs to make sure that there is sufficient diversity among those groups or individuals being consulted, to ensure that all relevant perspectives are represented, and all relevant information is gathered.

3. Consultation and analysis

[170] ICO Handbook, Part I, Chapter I.
[171] Phases or tasks may be compressed or consolidated in the case of small-scale PIAs.
[172] A list of contents is provided in the ICO Handbook.

Phase 3 involves consultations with stakeholders, risk analysis, problem recognition and a search for solutions.

4. Documentation

This phase focuses on documenting the PIA process and its results (primarily in the form of a PIA report). The Handbook says a **PIA report** should be written with the expectation that it will be published, or at least be widely distributed.[173] The ICO Handbook sets out the following reasons for preparing a PIA report:

- as an element of accountability, in order to demonstrate that the PIA process was performed appropriately;
- to provide a basis for post-implementation review;
- to provide a basis for audit;
- to provide corporate memory, ensuring that the experience gained during the project is available to those completing new PIAs if original staff have left; and,
- to enable the experience gained during the project to be shared with future PIA teams and others outside the organisation.

It also sets out the key elements of a PIA report:

- a description of the project;
- an analysis of the privacy issues arising from it;
- the business case justifying privacy intrusion and its implications;
- a discussion of alternatives considered and the rationale for the decisions made;
- a description of the privacy design features adopted to reduce and avoid privacy intrusion and their implications of these design features;
- an analysis of the public acceptability of the scheme and its applications.

The Handbook says that if information collected during the PIA process is commercially or security sensitive, it could be redacted or placed in confidential appendices, if justifiable.

5. Review and audit

The purpose of this phase is to ensure that the organisation implements the undertakings arising from the consultation and analysis phase and are effective.

In Chapter II, the Handbook explains that **privacy risks** fall into two categories:

i. Risks to the individual as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information.
ii. Risks to the organisation as a result of:
    - perceived harm to privacy;
    - a failure to meet public expectations on the protection of personal information;
    - retrospective imposition of regulatory conditions;
    - low adoption rates or poor participation in the scheme from both the public and partner organisations;
    - the costs of redesigning the system or retro-fitting solutions;
    - collapse of a project or completed system;

[173] ICO, PIA Handbook, p. 40.

- withdrawal of support from key supporting organisations due to perceived privacy harms; and/ or
- failure to comply with the law, leading to:
    - enforcement action from the regulator; or
    - compensation claims from individuals.

It then goes on to identify various privacy risks.

Once the organisation has identified and assessed the privacy risks, it has three options:

- accept the risks, impacts or liabilities;
- identify a way to avoid the risks (a privacy impact avoidance measure); or
- identify a way to mitigate the risks (a privacy impact mitigation measure).

Part II of the Handbook explicates in more detail **the PIA process**.

Chapter III – **Initial assessment** aims to help organisations determine if a PIA is needed. The Handbook says three pieces of information are needed: a project outline; a stakeholder analysis; and an environmental scan. The purpose of the screening process is to ensure that the investment the organisation makes is proportionate to the risks involved. The Handbook offers four sets of questions to indicate whether a PIA is needed, and if so, whether the project requires a full-scale PIA, a small-scale PIA or just a check against compliance with the law.

Full-scale PIA: This is a more comprehensive internal privacy risk assessment in cases where there is a chance of a substantial privacy impact. A full-scale PIA encompasses privacy risk analysis, stakeholder consultation and proposal of solutions to the risks. The criteria for determining if a full-scale PIA is required are set out in Appendix 1 of the Handbook. The criteria are set out as questions, the answers to which, when considered as a whole, would indicate whether a full-scale PIA is warranted.

Small-scale PIA: This is a less formal version of a full-scale PIA, involving less investment and fewer resources, less exhaustive analysis and information gathering and generally used to study specific project aspects. In a small-scale PIA, says the Handbook, consultation does not have to be a formal process and can be limited to the stakeholders who have a key interest in the project or those who may have the biggest concerns about the project. It may, depending on the size of the project, be limited to a meeting or workshop with the key stakeholders, a series of short telephone interviews or even involve simply writing to the key stakeholders. The key deliverable is a document (such as a privacy design features paper or a meeting outcomes report) that details the privacy impacts identified[174] and the solutions or actions which will be taken to deal with them. This document must be in a form which can be published and provided to the various parties involved in the consultation.

Privacy law compliance check: This check determines whether the project complies with privacy and data protection laws such as the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and the Data Protection Act 1998. Private sector organisations will also have to consider industry standards and law. Further documents may be relevant, such as codes of conduct and privacy policy statements. The organisation proposing the project is responsible for undertaking a survey of the law relevant to the project and to the data processing and business processes it gives rise to.

[174] ICO, PIA Handbook, p. 46.

Data protection compliance checklist: This is generally carried out after implementation of the project and is a checklist for compliance with the Data Protection Act 1998.

Review and re-do: This stage envisages a timetable for reviewing actions taken after the PIA and their effectiveness. It also envisages checking whether new aspects of projects might be subject to a PIA.

* * *

The following table lists the key points – the "touch points" – in the ICO PIA Handbook, which can be compared to the touch points in other PIA methodologies, to identify similarities in the processes.

	Touch points from the PIA Handbook	Key points from other PIA methodologies or PIA reports
1	PIAs must comply with (more than just data protection) legislation. Private sector organisations will also have to consider industry standards, codes of conduct and privacy policy statements.	
2	PIA is a process.	
3	A PIA could consider: 1. privacy of personal information; 2. privacy of the person; 3. privacy of personal behaviour; and 4. privacy of personal communications.	
4	PIA should be undertaken when it is possible to influence the development of a project.	
5	Responsibility for the PIA should rest at the senior executive level.	
6	The organisation should develop a plan for the PIA and its terms of reference. It should develop a consultation strategy appropriate to the scale, scope and nature of the project.	
7	A PIA should include an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources).	
8	The organisation should determine whether a small-scale or full-scale PIA is needed.	
9	A PIA should seek out and engage stakeholders internal and external to the organisation. The assessor needs to make sure that there is sufficient diversity among those groups or individuals being consulted, to ensure that all relevant perspectives are	

	Touch points from the PIA Handbook	Key points from other PIA methodologies or PIA reports
	represented, and all relevant information is gathered.	
10	The organisation should put in place measures to achieve clear communications between senior management, the project team and representatives of, and advocates for, the various stakeholders.	
11	The PIA should identify risks to individuals and to the organisation.	
12	The organisation should identify less privacy-invasive alternatives. It should identify ways of avoiding or minimising the impacts on privacy or, where negative impacts are unavoidable, clarify the business need that justifies them.	
13	The organisation should document the PIA process and publish a report of its outcomes.	
14	A PIA report should be written with the expectation that it will be published or at least be widely distributed. The report should be provided to the various parties involved in the consultation. If information collected during the PIA process is commercially or security sensitive, it could be redacted or placed in confidential appendices, if justifiable.	
15	The PIA should be re-visited in each new project phase.	
16	A PIA should be subject to third-party review and audit, to ensure the organisation implements the PIA recommendations.	

6.2 KEY FEATURES FROM THE RFID PIA FRAMEWORK

The Privacy and Data Protection Impact Assessment Framework for RFID Applications, dated 12 January 2011,[175] was endorsed by the Article 29 Working Party on 11 February 2011 in its Working Paper 180,[176] and signed by the EC on 6 April 2011. This culminated two years of chequered development that saw the PIA's first draft rejected by the Article 29 Working Party in Working Paper 175,[177] and revised to meet the criticism of its deficiencies.

[175] http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf
[176] Article 29 Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, Adopted 11 February 2011.
[177] Article 29 Working Party, Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact

The genesis of the RFID PIA Framework was in 2009 when the EC recommended that industry develop a framework for this technology, radio frequency identification,[178] which is widely used to track the location of objects or persons, and which is perceived as posing a threat to individual privacy. The Opinions of the Article 29 Working Party, as well as other relevant literature by "insiders" to the process who describe the history of the Framework and discuss its contents, should be read in conjunction with the present account.[179]

The 24-page Framework is a high-level document for RFID "application operators" to adapt in conducting PIAs relevant to the circumstances and contexts of their use of RFID. Benefits of conducting an RFID PIA flow from being able to:

- establish and maintain compliance with privacy and data protection laws and regulations;
- manage risks to its organisation and to users of the RFID Application (both privacy and data protection compliance-related and from the standpoint of public perception and consumer confidence); and
- provide public benefits of RFID Applications while evaluating the success of privacy by design efforts at the early stages of the specification or development process.

The Framework focuses on "privacy and data protection", implicitly differentiating between these two concepts or aims. This is significant in that the analytical technique adopted in the Framework is aligned to *data protection* and its well-known principles; "privacy" is undefined but apparently assumed to result from compliance with the requirements of data protection.

The Framework outlines internal procedures by which application operators should support the conduct of PIA; in abbreviated form, they are:

- Scheduling of the PIA process
- Internal review of the PIA process (including the initial analysis) and PIA reports
- Compilation of supporting artefacts
- Determination of the persons and/or functions within the organisation who have the authority for relevant actions
- Provision of criteria for how to evaluate and document whether the application is ready or not ready for deployment
- Consideration or identification of factors that would require a new or revised PIA report
- Stakeholder consultation.

The PIA process itself has two phases:

1. Initial Analysis Phase: the RFID Application Operator will follow…steps…to

---

Assessment Framework for RFID Applications, Adopted 13 July 2010.

[178] Described on p. 23 of the Framework glossary as "[t]he use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it."

[179] See Spiekermann, Sarah, "The RFID PIA Developed by Industry, Endorsed by Regulators", Chapter 15, and Beslay, Laurent, and Anne-Christine Lacoste, "Double-Take: Getting to the RFID PIA Framework", Chapter 16, in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, pp. 323-346; pp. 347-359.

determine:
a) whether a PIA of its RFID application is required or not; and
b) if a full or small scale PIA is warranted.

2. Risk assessment phase: it outlines the criteria and elements of full and small scale PIAs.

A decision tree assists the first phase; the initial analysis "must be documented and made available to data protection authorities upon request", and Annex I shows the items of information that should be included in this. The Framework then describes full-scale and small-scale PIAs before explaining the second phase, the objective of which "is to identify the privacy risks caused by an RFID Application – ideally at an early stage of system development – and to document how these risks are *pro-actively* mitigated through technical and organisational controls." [Emphasis in original.] This serves a further purpose, that of showing the application's compliance with the legal requirements of privacy as set forth in Directive 95/46/EC and thereby helping to judge the effectiveness of mitigation. Risk assessment is conceived in the standard manner, as consisting of assessments of the likelihood and magnitude of consequences. The adherence of the PIA Framework to the legal requirements of the Directive is reinforced by its advice that operators should use the nine "privacy targets" embedded in the Directive as their starting-point in assessing risk. Annex II itemises these targets; in its words:

- Safeguarding quality of personal data
- Legitimacy of processing personal data
- Legitimacy of processing *sensitive* personal data
- Compliance with the data subject's right to be informed
- Compliance with the data subject's right of access to data, correct and erase data
- Compliance with the data subject's right to object
- Safeguarding confidentiality and security of processing
- Compliance with notification requirements
- Compliance with data retention requirements.

Meeting these targets gives the impression that the Framework is concerned particularly with data-protection *compliance*, although the PIA process "aims to consider all potential risks and then reflects on their magnitude".[180] The PIA process requires the application operator to undertake four steps:

1. Describe the RFID Application [see Annex I of the Framework];
2. Identify and list how the RFID Application under review could threaten privacy and estimate the magnitude and likelihood of those risks;
3. Document current and proposed technical and organisational controls to mitigate

[180] Spiekermann writes: "The PIA Framework consortium took the articles of the Data Protection Directive as its privacy targets for several reasons. Most importantly, it is very useful and sensible to draw privacy threats from existing legal frameworks and thereby combine a PIA with a legal compliance check. While scholars tend to distinguish PIAs from compliance checks and privacy audits, the stakeholder negotiation over RFID PIAs cast doubt on the value of this distinction: taking privacy legislation as a starting point for privacy threat analysis saves companies cost and time." She also gives other reasons that are in keeping with this pragmatism, but remarks that "taking legislation as the privacy target for PIA also has drawbacks. One is that the data protection laws may not cover all of the privacy issues inherent in RFID", such as the right to be let alone and people's fears of "being restricted, criticised or exposed through automatic object reactions". See Spiekermann, Sarah, "The RFID PIA – Developed by Industry, Endorsed by Regulators", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, pp. 337-339.

identified risks; and

4. Document the resolution (results of the analysis) regarding the application.

For step 2, Annex III of the Framework lists potential privacy risks, as follows:

- Unspecified and unlimited purpose
- Collection exceeding purpose
- Incomplete information or lack of transparency
- Combination exceeding purpose
- Missing erasure policies or mechanisms
- Invalidation of explicit consent
- Secret data collection by the RFID Operator
- Inability to grant access
- Prevention of objections
- A lack of transparency of automated individual decisions
- Insufficient access right management
- Insufficient authentication mechanism
- Illegitimate data processing
- Insufficient logging mechanism
- Uncontrollable data gathering from RFID tags.

These "privacy risks" are conceived in *procedural* terms, derivative from legal data-protection requirements, and there is little direct attempt to characterise privacy risks in terms of *substantive* threats to the privacy of the individual data subject that could be mitigated or prevented.[181] Nevertheless, the Framework requires operators to consider the significance of a risk and the likelihood of its occurrence, as well as the magnitude of the impact; the resulting level of risk could be classified as low, medium or high, although the Framework gives no guidance about the criteria or the procedures for making these judgements. The question of the deactivation of RFID tags by retailers after the point of sale, which featured in the Article 29 Working Party criticisms, is addressed as part of operators' necessary risk assessment.

The Framework discusses step three, the identification and recommendation of controls to minimise, mitigate or eliminate the privacy risks. There are technical and non-technical (management and operational) controls, and controls can be preventive or detective. Some controls are considered "natural" in the environment of the RFID: for example, the absence of tag-readers obviates risk. Annex IV gives a long list of categorised examples of controls, including accountability measures. Step four is the final one: documentation of resolution and residual risks, after which the PIA report can be written, including a description of the RFID application (Annex I) and documentation of the four steps. However, its publication may be restricted for reasons of commercial confidentiality and security.

The following table shows where the Framework has followed the ICO PIA Handbook guidance.

[181] An example of the latter approach may be found in the GIRFEC PIA, described elsewhere in this Report in Annex 1 at section 6.5. The GIRFEC PIA identifies, and shows ways of mitigating, eight risks within its field of activity.

	Touch points extracted from the ICO PIA Handbook	RFID PIA Framework
1	PIAs must comply with (more than just data protection) legislation. Private sector organisations will also have to consider industry standards, codes of conduct and privacy policy statements.	The Framework does not indicate this but it is likely. It says: "The PIA Framework is part of the context of other information assurance, data management, and operational standards that provide good data governance tools for RFID and other Applications." Compliance with Directive 95/46/EC is emphasised in several places, and the Directive serves as a touchstone.
2	PIA is a process.	Yes.
3	A PIA could consider: • privacy of personal information; • privacy of the person; • privacy of personal behaviour; and • privacy of personal communications	The privacy of personal information is paramount in this PIA, which is closely aligned with data protection and its principles; other types are not involved.
4	PIA should be undertaken when it is possible to influence the development of a project.	Yes.
5	Responsibility for the PIA should rest at the senior executive level.	The Framework says: "Within companies, individuals…designated with responsibility for overseeing and assuring organisational or departmental privacy… are essential participants in the PIA process. …Employees with knowledge of technical, marketing and other disciplines may also be needed participants in the process."
6	The organisation should develop a plan for the PIA and its terms of reference. It should develop a consultation strategy appropriate to the scale, scope and nature of the project.	This has been accomplished.
7	A PIA should include an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources).	Not specified.
8	The organisation should determine whether a small-scale or full-scale PIA is needed.	Yes.
9	A PIA should seek out and engage stakeholders internal and external to the organisation. The assessor needs to make sure that there is sufficient diversity among those groups or individuals being consulted, to ensure that all relevant perspectives are represented, and all relevant information is gathered.	Yes, but some of this is implicit and vague.
10	The organisation should put in place	Not addressed.

	Touch points extracted from the ICO PIA Handbook	RFID PIA Framework
	measures to achieve clear communications between senior management, the project team and representatives of, and advocates for, the various stakeholders.	
11	The PIA should identify risks to individuals and to the organisation.	Risks to the individual are identified (largely procedural and related to data protection principles), but not to the organisation (the RFID application operator).
12	The organisation should identify less privacy-invasive alternatives. It should identify ways of avoiding or minimising the impacts on privacy or, where negative impacts are unavoidable, clarify the business need that justifies them.	To an extent, e.g., with the question of deactivation of RFID tags.
13	The organisation should document the PIA process and publish a report of its outcomes.	Heavy emphasis on documentation. About publication, the Framework says the Report: "is made available to competent authorities". It is not clear who the "competent authorities" are.
14	A PIA report should be written with the expectation that it will be published, or at least be widely distributed. The report should be provided to the various parties involved in the consultation. If information collected during the PIA process is commercially or security sensitive, it could be redacted or placed in confidential appendices, if justifiable.	The Framework says: "Proprietary and security sensitive information may be removed from PIA Reports before the Reports are provided externally (e.g., to the competent authorities) as long as the information is not specifically pertinent to privacy and data protection implications. The manner in which the PIA should be made available (e.g., upon request or not) will be determined by member states. In particular, the use of special categories of data may be taken into account, as well as other factors such as the presence of a data protection officer."
15	The PIA should be re-visited in each new project phase.	The need for revision is explicitly discussed.
16	A PIA should be subject to third-party review and audit, to ensure the organisation implements the PIA recommendations.	Audit is not mentioned. Implementation is mentioned, but not discussed.

6.3 KEY FEATURES FROM ARTICLE 33 OF THE PROPOSED DATA PROTECTION REGULATION

The European Commission officially released its package for reform of the data protection framework in Europe on 25 January 2012. The centrepiece of the reform package was the proposed Data Protection Regulation,[182] Article 33 of which would make privacy impact assessment (the Regulation uses the term "data protection impact assessment") mandatory "where processing operations present specific risks to the rights and freedoms of data subjects [individuals]". Article 33 goes further than any other PIA policy, in making PIA mandatory for all organisations, from both the public and private sectors, wherever they present a risk to data subjects.

Article 33 is reproduced here for ease of reference.

Data protection impact assessment

1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
2. The following processing operations in particular present specific risks referred to in paragraph 1:
(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;
(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;
(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;
(d) personal data in large scale filing systems on children, genetic data or biometric data;
(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).
3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.
4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.
5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.

[182] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", COM(2012) 11 final, Brussels, 25 January 2012. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.
7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 33 should be read in conjunction with recitals 70-74. For example, recital 74 says that data controllers should consult the supervisory authority "prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation".

Article 33 sets out examples of specific risks, including processing involving evaluation of a person's economic situation, location, health, personal preferences, reliability or behaviour, sex life, health, race and ethnic origin; video surveillance; genetic or biometric data; or other processing operations requiring consultation with the data protection authority.

Article 33 briefly describes what a PIA report shall contain – "at least" a general description of the envisaged processing operations, an assessment of the risks to data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation.

Interestingly, the proposed Regulation would require data controllers to seek the views of data subjects or their representatives on the intended processing.

The PIA requirements described in Article 33 are rather sketchy, hence, the Commission includes a provision that would empower it to specify additional criteria and conditions at a later time, including conditions for "scalability, verification and auditability". It would also be empowered to specify standards and procedures for carrying out, verifying and auditing PIAs.

The provisions of Article 33 have generally been supported by data protection authorities across Europe, as represented in the Article 29 Data Protection Working Party. In its March 2012 Opinion,[183] the Working Party said it "welcomes the inclusion of provisions that give incentives to controllers to invest, from the start, in getting data protection right (such as data protection impact assessments, data protection by design and data protection by default). The proposals place clear responsibility and accountability on those processing personal data."

While the Working Party welcomed the obligation to carry out a PIA, it had some specific suggestions for improvement of Article 33. It felt that a PIA should also be done "when it is not clear whether the processing would present specific risks". Thus, the Working Party suggested that Article 33 be slightly amended to read "Where processing operations *are likely to* present specific risks…".[184]

[183] Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, Brussels, 23 March 2012. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
[184] Ibid., p.16. Italics added.

In addition, the Art. 29 WP suggested that the limitation under Article 33 to processing "on a large scale" should be deleted, as the Working Party believes that a PIA should be "required for such processing operations even on a small scale". Here, as elsewhere, the Art. 29 WP is of the view that PIAs should be used even more widely than proposed by the Commission. The Working Party comments: "This is especially true for the processing of biometric data, which the Working Party feels under certain circumstances should be considered risky and therefore a data protection impact assessment should be carried out irrespective of any thresholds provided for in Article 33. Also, … the exception for public authorities in Article 33(5) to carry out an impact assessment is unjustified, unless such an assessment has already been carried out during the legislative process."

As further evidence of DPAs' wishing to see wider use of privacy impact assessments than proposed by the Commission, the Art. 29 WP urges the Commission to include in the proposed Directive for data protection in the area of police and justice (which was part of the same reform package as the proposed Regulation) a provision requiring a privacy impact assessment during the legislative procedure. The Working Party opined that "these are particularly important in the field of law enforcement processing of personal data, given the increased risks to individuals of this processing".

Data protection authorities also clearly believe in sharing information amongst themselves on favourable decisions taken on data protection impact assessments.

Even taking into account the amendments suggested by the Article 29 Working Party, Article 33 still leaves some questions unanswered. For example, should PIA reports be published? Should PIAs be audited? Should there be a central registry of PIA reports? Should PIA reports be submitted to the data protection authorities (DPAs)? Should a PIA conducted in one Member State be recognised in another Member State?

An important shortcoming of Article 33 is its focus on data protection, rather than privacy. Hence, its narrow focus could mean that infringements of other types of privacy (e.g., privacy of communications, privacy of location, privacy of behaviour) would be ignored.

It is perhaps unfair to compare a one-page Article 33 with an 86-page PIA Handbook, nevertheless, it is useful to see how many points Article 33 bears in common with the Handbook.

	Touch points from the PIA Handbook	**Touch points from Article 33**
1	PIAs must comply with (more than just data protection) legislation. Private sector organisations will also have to consider industry standards, codes of conduct and privacy policy statements.	Not mentioned.
2	PIA is a process.	The wording of Article 33(3) seems to emphasise the report rather than the process: "The assessment shall contain at least a general description…".
3	A PIA could consider: • privacy of personal information; • privacy of the person;	Article 33 focuses only on the first item, i.e., data protection. This is a serious shortcoming.

	Touch points from the PIA Handbook	Touch points from Article 33
	• privacy of personal behaviour; and • privacy of personal communications.	
4	PIA should be undertaken when it is possible to influence the development of a project.	Article 33(1) implies this. It says the DPIA shall be carried to assess the impact of the "envisaged" operations.
5	Responsibility for the PIA should rest at the senior executive level.	Not mentioned.
6	The organisation should develop a plan for the PIA and its terms of reference. It should develop a consultation strategy appropriate to the scale, scope and nature of the project.	Not mentioned.
7	A PIA should include an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources).	Not mentioned.
8	The organisation should determine whether a small-scale or full-scale PIA is needed.	Not mentioned.
9	A PIA should seek out and engage stakeholders internal and external to the organisation. The assessor needs to make sure that there is sufficient diversity among those groups or individuals being consulted, to ensure that all relevant perspectives are represented, and all relevant information is gathered.	Article 33(4) says the data controller shall seek the views of data subjects.
10	The organisation should put in place measures to achieve clear communications between senior management, the project team and representatives of, and advocates for, the various stakeholders.	Not mentioned.
11	The PIA should identify risks to individuals and to the organisation.	Article 33(2) mentions specific risks. Hence, the wording is not optimum for identifying risks others than those specifically mentioned in the article.
12	The organisation should identify less privacy-invasive alternatives. It should identify ways of avoiding or minimising the impacts on privacy or, where negative impacts are unavoidable, clarify the business need that justifies them.	Not mentioned.
13	The organisation should document the PIA process.	Not mentioned.

	Touch points from the PIA Handbook	Touch points from Article 33
14	A PIA report should be written with the expectation that it will be published, or at least be widely distributed. The report should be provided to the various parties involved in the consultation. If information collected during the PIA process is commercially or security sensitive, it could be redacted or placed in confidential appendices, if justifiable.	Article 33 envisages production of a report but is silent on whether the report should be published in whole or in part.
15	The PIA should be re-visited in each new project phase.	Not mentioned.
16	A PIA should be subject to third-party review and audit, to ensure the organisation implements the PIA recommendations.	Article 33 would empower the Commission to adopt delegated acts including those relating to verifying and auditing the DPIA.

6.4 KEY FEATURES OF THE PIAF METHODOLOGY

The purpose of the PIAF project was to review PIA practices and methodologies in those countries with the most experience and to identify good practices that could inform recommendations for an optimised PIA for Europe. The PIAF project (PIAF stands for Privacy Impact Assessment Framework), funded by the European Commission's Directorate-General Justice,[185] began in January 2011 and finished at the end of October 2012. The project had three main phases. In the first phase, the consortium examined various PIA policies and methodologies from Australia, Victoria state, Canada, Ontario, Alberta, Hong Kong, Ireland, New Zealand, the UK and the US, with a view to identifying the best elements of each. In the second phase, the consortium sent a survey to European data protection authorities asking for their views on some of the key elements and issues associated with PIA policy. In the third phase, the consortium prepared a set of recommendations for an "optimised" PIA framework based on their findings and conclusions from the previous phases.

Several data protection authorities said in their responses to the PIAF questionnaire that they preferred a streamlined, short, easy-to-understand and easy-to-use methodology. Hence, PIAF produced a six-page "Step-by-step guide to privacy impact assessment" and a six-page "Template for a privacy impact assessment report".[186]

The consortium distinguished between a PIA *process* and a PIA *report*. A report is meant to document the PIA process, but in fact the PIA process extends beyond a PIA report. Even after the PIA assessor or team produce their report, which in most cases should contain recommendations, someone will need to make sure the recommendations are implemented or, if some are not, explain why they are not.

[185] The PIAF consortium comprised Vrije Universiteit Brussel (Belgium), Trilateral Research & Consulting (UK), and Privacy International (UK). In addition to a review of PIA methodologies, the PIAF report includes an analysis of 10 PIA reports, two each from Australia, Canada, New Zealand, the UK and US. To our knowledge, this is the first such review of actual PIA reports from these countries.

[186] Both papers can be found here: http://www.piafproject.eu/Events.html

Hence, the first document, the "Step-by-step guide" is a guide to the PIA process, while the other suggests what a PIA report should contain. The PIAF consortium prepared both documents based on their review of existing PIA methodologies. The next section highlights the key elements in the optimised PIA process recommended by PIAF.

Drawing on the best practices of existing PIA methodologies, the "Step-by-step guide to privacy impact assessment" contains 16 principal steps in the PIA process, as set out below. These steps are set out somewhat succinctly as those in an "optimised" PIA process. Some less than optimal PIAs may not follow all of these steps and some may follow them in variations of the sequence set out here. However, we regard the steps below as generally necessary if a PIA is to have "teeth", if the PIA is to be effective in identifying and minimising or avoiding privacy risks. "Generally" is the operative word. If the privacy risk is regarded as relatively trivial, affecting only a few people, it may not be necessary to follow all of the steps set out below (e.g., it may not be necessary to consult external stakeholders or even to publish the PIA report). At the end of each step, we identify which countries promote such steps.

1. Determine whether a PIA is necessary (threshold analysis)

Generally, if the development and deployment of a new project (or technology, service…) impacts upon privacy, the project manager should undertake a PIA. A PIA should be undertaken when it is still possible to influence the design of a project or, if the project is too intrusive upon privacy, the organisation may need to decide to cancel the project altogether rather than suffer from the negative reaction of consumers, citizens, regulatory authorities, the media and/or advocacy gadflies. Australia, Victoria state, Canada, Ontario, Alberta, Ireland and the US (DHS) use threshold analyses (typically a small set of questions) to determine whether a PIA should be conducted. The UK uses a threshold analysis to determine whether a "full-scale" or "small-scale" PIA should be conducted.

2. Identify the PIA team and set the team's terms of reference, resources and time frame

The project manager should be responsible for the conduct of a PIA, but she may need some additional expertise, perhaps from outside her organisation. The project manager and/or the organisation's senior management should decide on the terms of reference for the PIA team, its nominal budget and its time frame. The terms of reference should spell out whether public consultations are to be held, to whom the PIA report is to be submitted, whether the PIA report is to be published. The UK especially recommends this step. The minimum requirements for a PIA will depend on how significant an organisation deems the privacy risks to be. That an organisation may well downplay the seriousness of the risks makes third-party review and/or audit (see step 14) necessary.

3. Prepare a PIA plan

The plan should spell out what is to be done to complete the PIA, who on the PIA team will do what, the PIA schedule and, especially, how the consultation will be carried out. It should specify why it is important to consult stakeholders in this specific instance, who will be

consulted and how they will be consulted (e.g., via public opinion survey, workshops, focus groups, public hearings, online experience…). Australia and the UK explicitly advocate preparation of plans for a PIA. Some countries, including Australia and the UK, say there is no "one size fits all" for PIA reports, while others, such as Alberta and Ireland, provide templates for such reports. If the regulator does not specify a PIA template, we encourage organisations to follow the PIA process advocated here and the PIA report template which can be found on the PIAF website.

4. Agree the budget for the PIA

Once the project manager and/or assessor have prepared a PIA plan, they can estimate the costs of undertaking the PIA and seek the budgetary and human resources necessary from the organisation's senior management. Their plan may require an increase in the nominal budget initially set by senior management or the assessor may need to revise her PIA plan based on the budget available. If the assessor is unable to do an adequate PIA, she should note this in her PIA report.

5. Describe the proposed project to be assessed

The description can be used in at least two ways – it can be included in the PIA report and it can be used as a briefing paper for consulting stakeholders. The description of the project should provide some contextual information (why the project is being undertaken, who comprises the target market, how it might impact the consumer-citizen's privacy, what personal information will be collected). The project description should state who is responsible for the project. It should indicate important milestones and, especially, when decisions are to be taken that could affect the project's design. All existing PIA methodologies include this step.

6. Identify stakeholders

The assessor should identify stakeholders, i.e., those who are or might be interested in or affected by the project, technology or service. The stakeholders could include people who are internal as well as external to the organisation. They could include regulatory authorities, customers, citizen advocacy organisations, suppliers, service providers, manufacturers, system integrators, designers, academics and so on. The assessor should identify these different categories and then identify specific individuals from within each of the categories, preferably as representative as possible. The range and number of stakeholders to be consulted should be a function of the privacy risks and the assumptions about the frequency and consequences of those risks and the numbers of citizen-consumers who could be impacted. Australia, Victoria state, Ireland and the UK take this step.

7. Analyse the information flows and other privacy impacts

The assessor should consult with others in the organisation and perhaps external to the organisation to describe the information flows and, specifically, who will collect what information from whom for what purpose; how will the organisation use the collected information; how will the information be stored, secured, processed and distributed (i.e., to whom might the organisation pass on the information), how well will secondary users (e.g., the organisation's service providers, apps developers) protect that information or will they pass it on to still others? This analysis should be as detailed as possible to help identify

potential privacy risks. The assessor should consider the impacts not only on information privacy, but other types of privacy as well. Australia, Victoria state, Canada, Ontario, Alberta, Ireland and New Zealand say that a PIA should describe information flows. This step could be taken immediately after step 5 and concurrently with step 6.

8. Consult with stakeholders

There are many reasons for doing so, not least of which is that they may identify some privacy risks not considered by the project manager or assessor. By consulting stakeholders, the project manager may forestall or avoid criticism that they were not consulted. If something does go wrong downstream – when the project or technology or service is deployed – an adequate consultation at an early stage may help the organisation avoid or minimise liability. Furthermore, consulting stakeholders may provide a sort of "beta test" of the project or service or technology. Consulted stakeholders are less likely to criticise a project than those who were not consulted. Australia, Victoria state, Ireland and the UK urge consultation with stakeholders. This step could be taken after step 5, but it would be better after step 7, since the latter may uncover additional privacy risks not apparent after only step 5.

9. Check the project complies with legislation

A privacy impact assessment is more than a compliance check, nevertheless, the assessor or her legal experts should ensure that the project complies with any legislative or regulatory requirements. Australia, Victoria state, Canada, Ireland, New Zealand, the UK and the US note the importance of this step.

10. Identify risks and possible solutions

The assessor and her PIA team, preferably through stakeholder consultation, should identify all possible risks, who those risks will impact and assess those risks for their likelihood (frequency) and consequence (magnitude of impact) as well as the numbers of people who could be affected. Assessing risks is a somewhat subjective exercise. Thus, the assessor will benefit from engaging stakeholder representatives and experts to have their views. Deciding how to mitigate or eliminate or avoid or transfer the risk is also a somewhat political decision as is the decision regarding which risks to retain. All PIA methodologies feature this step. Information security risks, such as those contained in ISO 27005[187], do not address specific privacy risks. Hence, some PIA methodologies, e.g., those of Australia, Victoria state, Canada Alberta, Ontario and New Zealand, mention specific privacy risks.

11. Formulate recommendations

The assessor should be clear to whom her recommendations are directed – some could be directed towards different units within the organisation, some to the project manager, some to the CEO, some to employees or employee representatives (e.g., trade unions), to regulatory authorities, third-party apps developers, etc. If stakeholders have sight of draft recommendations, before they are finalised, they may be able to suggest improvements to existing recommendations or make additional ones. All PIA methodologies call for recommendations.

[187] http://www.iso.org/iso/catalogue_detail?csnumber=56742

12. Prepare and publish the report, e.g., on the organisation's website

Some organisations may be afraid to publish their PIAs because they fear negative publicity or they have concerns about competitors learning something they don't want them to. Such concerns seem overdone. There are solutions. The organisation can simply redact the sensitive bits or put them into a confidential annex. As in Step 11, if the assessor gives stakeholders sight of the draft PIA report, they may be able to suggest improvements before it is finalised. Australia and Ireland encourage publication, the US requires it. Canada publishes summaries.

13. Implement the recommendations

The project manager and/or the organisation may not accept all of the PIA recommendations, but they should say which recommendations they are implementing and why they may not implement others. The organisation's response to the assessor's recommendations should be posted on the organisation's website. This transparency will show that the organisation treats the PIA recommendations seriously, which in turn should show consumers and citizens that the organisation merits their trust. Canada, Ireland, New Zealand and the UK say a PIA report should justify any remaining risks. Victoria state says an organisation will need to consider how residual risks will be managed.

14. Third-party review and/or audit of the PIA

Existing PIA reports are of highly variable quality, from the thoughtful and considered to the downright laughable. Some PIA reports exceed 150 pages, others are only a page and a half in length, the sheer brevity of which makes them highly suspect. Independent, third-party review and/or audits are the only way to ensure PIAs are properly carried out and their recommendations implemented. The Office of the Privacy Commissioner of Canada (OPC) has indicated and extolled the benefits of independent audits.[188] Data protection authorities do not have the resources to audit all PIAs, but they could audit a small percentage, enough to make organisations ensure their PIAs are reasonably rigorous. Alternatively, independent auditors could undertake this task, just as they audit a company's financial accounts. Yet another alternative would be for organisations such as the International Association of Privacy Professionals (IAPP) to certify privacy auditors. The Government Accountability Office (GAO) audits PIAs in the US. The DHS has built independent, third-party review into its PIA process. As mentioned above, the Office of the Privacy Commissioner audits PIAs in Canada. New Zealand also favours third-party review. The UK envisages review and audit of a PIA, but doesn't say who should do it.

15. Update the PIA if there are changes in the project

Many projects undergo changes before completion. Depending on the magnitude of the changes, the assessor may need to revisit the PIA as if it were a new initiative, including a

[188] Stoddart, Jennifer, "Auditing Privacy Impact Assessments: The Canadian Experience", Chapter 20, in David Wright and Paul De Hert (eds.), Privacy Impact Assessment, Springer, Dordrecht, 2012, pp. 419-436 [p. 419]: The OPC audit "was an important initiative, not only for its findings – many of which can be applied cross-jurisdictionally – but also for its salutary effects on PIA practices government-wide."

new consultation with stakeholders. Australia says a PIA may need to be revisited as a project progresses. So does Ontario, the UK and the US Office of Management and Budget (OMB).

16. Embed privacy awareness throughout the organisation and ensure accountability

The chief executive officer is responsible for ensuring that all employees are sensitive to the privacy implications, the possible impacts on privacy, of what they or their colleagues do. The CEO should be accountable to her supervisory board or shareholders for the adequacy of PIA. In Canada, PIA reports have to be signed off by a senior official (e.g., a deputy minister). Ireland also says PIA reports should be approved by senior management. In the US, the chief information officer or privacy officer is expected to review and sign off PIAs. Some PIA methodologies (e.g., Canada) explicitly say that organisations should provide guidance and training to managers and staff.

The following table lists the key points – the "touch points" – in the ICO PIA Handbook, which can be compared to the touch points in the PIAF step-by-step PIA guide.

	Touch points from the PIA Handbook	**Key points from the PIAF "Step-by-step guide"**
1	PIAs must comply with (more than just data protection) legislation. Private sector organisations will also have to consider industry standards, codes of conduct and privacy policy statements.	Step 9 says to "Check the project complies with legislation".
2	PIA is a process.	The PIAF guide distinguishes between the PIA process and a PIA report.
3	A PIA could consider: 1. privacy of personal information; 2. privacy of the person; 3. privacy of personal behaviour; and 4. privacy of personal communications.	Step 7 says a PIA should consider the impacts not only on information privacy but other types of privacy as well.
4	PIA should be undertaken when it is possible to influence the development of a project.	Step 1 says "A PIA should be undertaken when it is still possible to influence the design of a project".
5	Responsibility for the PIA should rest at the senior executive level.	Step 2 says "The project manager and/or the organisation's senior management should decide on the terms of reference for the PIA team, its nominal budget and its time frame." Step 16 states "The CEO should be accountable to her supervisory board or shareholders for the adequacy of PIA."
6	The organisation should develop a plan for the PIA and its terms of reference. It should develop a consultation strategy appropriate to the scale, scope and nature of the project.	Step 2, as noted above, says "The project manager and/or the organisation's senior management should decide on the terms of reference for the PIA team, its nominal budget and its time frame. The terms of reference should spell out whether public consultations are to be held, to whom the PIA report is to be submitted, the budget for the

	Touch points from the PIA Handbook	Key points from the PIAF "Step-by-step guide"
		PIA, the time frame, whether the PIA report is to be published." Step 3 adds that "The plan should spell out what is to be done to complete the PIA, who on the PIA team will do what, the PIA schedule and, especially, how the consultation will be carried out. It should specify why it is important to consult stakeholders in this specific instance, who will be consulted and how they will be consulted (e.g., via public opinion survey, workshops, focus groups, public hearings, online experience…)."
7	A PIA should include an environmental scan (information about prior projects of a similar nature, drawn from a variety of sources).	Step 5 says to "Describe the proposed project to be assessed" and that "The description of the project should provide some contextual information (why the project is being undertaken, who comprises the target market, how it might impact the consumer-citizen's privacy, what personal information will be collected)."
8	The organisation should determine whether a small-scale or full-scale PIA is needed.	Step 1 of the PIAF guide is to "Determine whether a PIA is necessary (threshold analysis)" and refers to the ICO PIA Handbook which uses a threshold analysis to determine whether a full-scale or small-scale PIA should be conducted. In the preamble, the PIAF guide states that "If the privacy risk is regarded as relatively trivial, affecting only a few people, it may not be necessary to follow all of the steps set out below (e.g., it may not be necessary to consult external stakeholders or even to publish the PIA report)."
9	A PIA should seek out and engage stakeholders internal and external to the organisation. The assessor needs to make sure that there is sufficient diversity among those groups or individuals being consulted, to ensure that all relevant perspectives are represented, and all relevant information is gathered.	Step 6 says to "identify stakeholders, i.e., those who are or might be interested in or affected by the project, technology or service. The stakeholders could include people who are internal as well as external to the organisation…. The assessor should identify … different categories and then identify specific individuals from within each of the category, preferably as representative as possible. The range and number of stakeholders to be consulted should be a function of the privacy risks and the assumptions about the frequency and consequences of those risks and the numbers of citizen-consumers who could be

	Touch points from the PIA Handbook	Key points from the PIAF "Step-by-step guide"
		impacted."
10	The organisation should put in place measures to achieve clear communications between senior management, the project team and representatives of, and advocates for, the various stakeholders.	Step 8 is about consulting with stakeholders, but it does not specifically refer to "clear communications".
11	The PIA should identify risks to individuals and to the organisation.	Step 10 says that "The assessor and her PIA team, preferably through stakeholder consultation, should identify all possible risks, who those risks will impact and assess those risks for their likelihood (frequency) and consequence (magnitude of impact) as well as the numbers of people who could be affected."
12	The organisation should identify less privacy-invasive alternatives. It should identify ways of avoiding or minimising the impacts on privacy or, where negative impacts are unavoidable, clarify the business need that justifies them.	Step 10 notes that "Deciding how to mitigate or eliminate or avoid or transfer the risk is also a somewhat political decision as is the decision regarding which risks to retain." Step 13 states that "The project manager and/or the organisation may not accept all of the PIA recommendations, but they should say which recommendations they are implementing and why they may not implement others."
13	The organisation should document the PIA process and publish a report of its outcomes.	The PIAF guide does not specifically refer to documenting the PIA process. However, Step 12 says to "publish the report, e.g., on the organisation's website."
14	A PIA report should be written with the expectation that it will be published, or at least be widely distributed. The report should be provided to the various parties involved in the consultation. If information collected during the PIA process is commercially or security sensitive, it could be redacted or placed in confidential appendices, if justifiable.	Step 12 says that if there are concerns about competitors learning something, "The organisation can simply redact the sensitive bits or put them into a confidential annex."
15	The PIA should be re-visited in each new project phase.	Step 15 says to "Update the PIA if there are changes in the project."
16	A PIA should be subject to third-party review and audit, to ensure the organisation implements the PIA recommendations.	Step 14 concerns third-party review and/or audit of the PIA. It states that "Independent, third-party review and/or audits are the only way to ensure PIAs are properly carried out and their recommendations implemented."

6.5 EXAMPLES OF PUBLICLY AVAILABLE PIA REPORTS

After a detailed search on the Internet, we identified 26 publicly available PIA reports in the UK, all of which bar two originate in the public sector. Of these, we have selected several for more detailed analysis, below. Our review of existing PIA reports helps to provide a view of how PIAs are currently practised by public and private organisations (one of the PIA reports cited below comes from the private sector.

Note that in summarising the PIA reports, we do not include a footnote citing every page from where we extracted some text. We do for some that are particularly important, but not all. Suffice it to say that the text, paraphrased, quoted or otherwise extracted, in the summaries comes from the summarised document, unless otherwise specified.

PIA of the Draft Communications Data Bill, 14 June 2012

The Home Office states that the purpose of the PIA[189] is to:

- consider the privacy impact of the proposed legislation (the Communications Data Bill);
- assess whether the capabilities implemented through this proposed legislation will be compliant with the Data Protection Principles (DPP) and the Data Protection Act 1998 (DPA).

The 25-page PIA report says it has followed the approach and guidelines recommended by the ICO; indeed, it says the ICO "was fully consulted on this PIA and it reflects their advice".
The Privacy Impact Statement goes on to say that "implementation of the proposed legislation is capable of being fully compliant with the Data Protection Principles and the Data Protection Act". The statement includes a subsection on subject access requests, wherein it is stated that "The Data Protection Act gives the subjects of data the right to request access by making a Subject Access Request (SAR). An exemption to this exists for personal data that is being processed on the grounds of national security or for the 'prevention or detection of crime'." The Home Office says that, although there is no statutory obligation on communications service providers (CSPs) to produce PIAs, "they will be strongly encouraged to do so, or provide alternative assurance".

PIA on smart metering implementation

This 27-page PIA report, produced by the Department of Energy and Climate Change (DECC), has an Introduction that sets out the gist of the dilemma posed by smart metering:

> Smart metering will result in a step change in the volume, granularity and accuracy of energy consumption data that is made available by electricity and gas meters. Consumers will have near-real time information on their energy consumption to help them control energy use, save money and reduce emissions. Suppliers will have access to accurate data for billing and to improve their customer service. Network operators will have better information upon which to manage and plan current activities and the move towards smart grids which support sustainable energy supply. The new opportunities that this data provides in terms of delivery of benefits also raise new questions about the protection of this data and consumers' rights to privacy.

[189] Home Office, Privacy Impact Assessment of the Draft Communications Data Bill, 14 June 2012. http://www.homeoffice.gov.uk/publications/counter-terrorism/comms-data-bill/communications-data-privacy-ia?view=Binary

The DECC states that it has developed this PIA "to ensure that as policy has developed, any perceived Privacy impacts have been identified and proposals developed to manage them". It pushes PIA practice outward to private sector stakeholders too: "This PIA should be seen as an umbrella document for the Smart Metering Implementation Programme as a whole. The Government would expect that separate PIAs on individual practices are undertaken by all data controllers, such as suppliers, network operators and third parties, involved in the processing of smart meter data, prior to the mass roll-out of smart metering." DECC appears to have sought out and engaged internal and external stakeholders. This is very much in the spirit of the ICO PIA Handbook. DECC also appears to have taken steps to ensure diversity among groups and individuals consulted and all relevant perspectives represented.

PIA on the use of Smart Metering data by Network Operators

This PIA report[190] is one of only two that we have discovered from industry. It comes from an industry association, the Energy Networks Association (ENA). The ENA is to be congratulated for making the PIA publicly available – it has good reasons for doing so, as it explains. The stated purpose of the 77-page PIA is to assess the privacy issues surrounding the use of smart meter data by network operators (NOs)[191] and identify measures that can be taken to mitigate stakeholder concerns. The ENA considered it important to carry out a PIA because of the sensitivity around privacy and smart metering data. The PIA report, prepared by Engage Consulting Ltd, demonstrates to stakeholders that the ENA and its members are taking the issue of privacy seriously. Engage says it identified stakeholders and constructed an engagement plan with them. It interviewed many stakeholders and sent questionnaires to others. Engage says it followed the ICO's general guidance in undertaking the PIA and sought advice from the ICO on how it can be applied to the rollout of smart metering.

PIA on the Police National Database

The Home Office established the IMPACT programme "to improve the ability of the police service to manage and share intelligence and other operational information, to prevent and detect crime and make communities safer". The Police National Database (PND) holds information on people (e.g., names, including organisations), objects (e.g., cars), locations (e.g., addresses) and events (e.g., crime reports).[192] The National Policing Improvement Agency (NPIA) initiated its PIA[193] even before PIAs became mandatory. In the Foreword of the 42-page PIA report of the IMPACT programme, the chief executive and IMPACT programme director say they "are conscious that the management and sharing of information could raise privacy concerns and we are keen to ensure that these are addressed as fully as possible". They add that "privacy has been considered throughout the work on the Police

[190] Engage Consulting Limited, Privacy Impact Assessment: Use of Smart Metering data by Network Operators, Energy Networks Association, October 2011. The copyright and other intellectual property rights in this document are vested in the Energy Networks Association.

[191] The term "network operator" (NO) has been used to cover both the transmission and distribution businesses of electricity and gas.

[192] As 1 Dec 2012, the NPIA ceased operations. Some of its functions were transferred to the College of Policing and others were transferred to the Home Office. Administration of the Police National Computer (PNC), of which the Police National Database (PND) is a part, was transferred to the Home Office.

[193] National Policing Improvement Agency (NPIA), IMPACT Programme: Police National Database – Privacy Impact Assessment Report, April 2009 [42 pages].
http://www.npia.police.uk/en/docs/Privacy_Impact_Assessment.pdf

National Database and will continue to be as the work progresses. The NPIA is committed to ensuring that privacy is continuously considered across the organisation, and in all aspects of the IMPACT Programme." Thus, they recognise the value of embedding privacy awareness across their organisation. The NPIA sought to be "privacy friendly", not just "privacy compliant", which is good practice.

PIA on the Police source and covert consolidated data system

This 23-page report[194] endorses the contention that "PIAs are extremely helpful in identifying potential privacy issues at an early stage". In the context of the present project, the report says it has three purposes:

- Identify and manage any risks that privacy issues represent to realising the intended benefits of a regional Source & Covert Authority Management system.
- Identify any necessary privacy features so these could be designed in now, rather than be subject to costly retro-fitting at a later stage.
- Allow privacy considerations to be built into the design from the outset to provide a foundation for a flexible and adaptable system, reducing the cost of future changes and ensuring a longer service life.

The report goes on to say that by assessing and managing privacy issues, it will

- increase public confidence in the way in which Forces collect and use personal information;
- ensure the project and Regional Forces consider the legal basis for the new system, any obligation in relation to the collection of the personal data and any prohibitions on the use of that information;
- prevent problems arising and hence avoid subsequent expense and disruption;
- assist with risk management;
- protect the reputation of the Regional Forces.

The report tracks closely the ICO Handbook.

PIA on the Five Country Conference Protocol on sharing fingerprint data

This PIA concerns a Five Country Conference (FCC) Protocol, an agreement for sharing fingerprint data between immigration authorities in the UK, Australia, Canada, New Zealand and the US.[195] Under this Protocol, each FCC country will check specific sets of fingerprints against fingerprint databases of the other FCC countries. In cases where fingerprints match, the countries will exchange additional information as is relevant, proportionate and lawful to exchange for their immigration and nationality purposes. The UK Border Agency (UK BA) says the arrangements reflected in the PIA report strike a fair balance between protecting the privacy rights of the individual and the interests of the wider public. It hints that this PIA might be unique: "We are not aware of its previous use in the UK in relation to international information exchange projects of this kind." The UK BA says it has "followed the general guidance of the Information Commissioner's Office in undertaking this process, and sought specific advice on how it can best be applied to this type of project". After considering the

[194] Hill, Geoff, Regional Collaboration: Source & Covert – Privacy Impact Assessment Report, Devon & Cornwall Constabulary, 10 April 2012. http://www.devon-cornwall.police.uk/YourRightInformation/FreedomInformation/Documents/RegionalSCPrivacyImpactAssR.pdf

[195] UK Border Agency, Report of a Privacy Impact Assessment conducted by the UK Border Agency in relation to the High Value Data Sharing Protocol amongst the immigration authorities of the Five Country Conference, undated. http://www.ukba.homeoffice.gov.uk/sitecontent/documents/aboutus/workingwithus/high-value-data-sharing-protocol/pia.pdf?view=Binary

recommendations of the Cabinet Office Data Handling Review and having received advice from the Information Commissioner's Office, the Ministry of Justice, and other interested parties, the UK BA decided to publish this PIA report in order to increase transparency and public understanding of this activity.

PIA on the eCare Inter-Agency Communication Tool

The purpose of this PIA[196] is stated as follows: "This Report summarise[s] the results of a Privacy Impact Assessment on the Scottish Government eCare iACT application, which enhances the existing eCare data sharing Framework with targeted messaging capabilities, to support the data sharing requirements of the Getting It Right For Every Child (GIRFEC) policy." The Scottish Government understands PIA as a cyclical process and as "a vehicle for **assessing and managing privacy risks and issues** arising from a project or scheme involved in data sharing or use of communications technology, and **communicating** these with data subjects and other **stakeholders**, to determine the business justification for privacy intrusion / data sharing; assess the acceptability of the project, provide assurance and support transparency and trust." (Emphasis in original.) The 116-page report refers to ICO guidance material as well as to the Scottish Government's *Identity Management and Privacy Principles*[197], which were not yet promulgated when the GIRFEC PIA was carried out but were published at about the same time as this PIA was completed. GIRFEC and iACT involve co-working and decision-making for vulnerable persons across diverse social care, health and other organisations working in multi-agency partnerships. Therefore, the nature of the sharing of sensitive data, and of the privacy issues that arise in this kind of public service, require a careful PIA, which this one aims to provide while the ICT system was being developed. The PIA report clearly describes the intricate flows of various types of information in and across organisations in the eCare project.

[196] Scottish Government, eCare Programme, eCare/GIRFEC Inter-Agency Communication Tool (iACT) Privacy Impact Assessment. www.scotland.gov.uk/eCare. The Scottish Government decided to close eCare in 2013; see http://www.scotland.gov.uk/Topics/Health/Quality-Improvement-Performance/eHealth/eCare. We believe that the GIRFEC PIA, which took place within eCare, is still an important document for inclusion in this report.
[197] http://www.scotland.gov.uk/Publications/2010/12/PrivacyPrinciples

7 ANNEX 2 -- RESPONSES TO THE TRILATERAL SURVEYS

Trilateral has conducted three surveys germane to this study. The first was conducted in May 2012, and was aimed at determining whether UK organisations are conducting PIAs and whether they experience fewer data breaches because they are, as a consequence of conducting PIAs, more careful with personal data.

The second survey was in support of our proposal to the ICO, and it was aimed at finding out which risk management methodologies UK organisations were using and whether respondents felt PIA could be integrated with their risk management practice.

The third survey was part of this study and expanded upon the first two surveys. Its purpose was to find out what percentage of responding organisations were conducting PIAs and how many they have conducted and whether PIA could be integrated in their project and risk management practices.

The results should be regarded as indicative rather than definitive or representative, because the sample size was too small in all three cases. However, the results from all three surveys are consistent with each other.

7.1 RESPONSES TO THE MAY 2012 SURVEY ON PIAS

In May 2012, Trilateral carried out a survey of 40 UK organisations – central government departments, NHS trusts and local authorities – to query their adoption and use of privacy impact assessments. The following questions were part of this short survey:

1. *Has your organisation conducted a PIA? If so, how many PIAs have you done?*
2. *Do you think you have experienced fewer data breaches and privacy complaints as a result of having conducted a PIA?*
3. *Have you done the PIA internally with your own resources or have you used external consultants?*
4. *Does your organisation have a data protection officer?*
5. *Are you aware of the fact that the proposed European Data Protection Regulation includes a provision (Article 33) regarding mandatory privacy impact assessments?*

We received 25 responses to the survey. The key findings from the survey are summarised below:

- 64% of the respondents (16 organisations) have done a PIA.
- Of the organisations that have done a PIA, 44% (seven organisations) could not say how many PIAs they have done, the remaining organisations have done a number of PIAs ranging from two to as many as 455 PIAs for a single organisation.
- Of those that have done a PIA, the majority, 75%, are uncertain whether they have, or they have not, experienced fewer data breaches as result of having done the PIA, while 12.5% believe that they have experienced fewer data branches and the remaining 12.5% that they have not.
- 94% of the respondents that have done a PIA have done it internally with their own resources, while only 6% (equivalent to one organisation) have employed external resources.

- The majority of respondents, 88%, have a data protection officer in their organisation and 84% are aware that the proposed European Data Protection Regulation includes a provision for mandatory privacy impact assessment.

7.2 RESPONSES TO THE NOVEMBER 2012 SURVEY ON RISK MANAGEMENT

Partly as background for the preparation of its proposal to the ICO, in late November 2012, Trilateral sent a new questionnaire to the 25 public entities who had responded to our May 2012 survey, asking about which risk management standard or methodology they follow and the prospects for integrating PIA as part of their risk management process. We asked the following questions:

1. *Does your organisation follow a particular risk management methodology (e.g., ISO 29100, ISO 27000, ISO 31000)? If so, which risk management standard do you use?*

2. *Does your organisation currently consider privacy risks in the context of your overall risk management process?*

3. *If not, do you think it would be possible to include privacy impact assessment (PIA) as part of your risk management process?*

4. *If relevant to your organisation, is there any collaboration between the risk manager and the data protection officer regarding privacy risks management?*

From e-mailing the second set of questions on 28 November 2013, we had responses from 16 of the 25 organisations. Following are some of the findings from that survey:

- All of the respondents follow different variations of established and externally developed risk management methodologies, often combined together, ranging from:
  - the Treasury's Orange Book as the main risk management guide and Her Majesty's Government (HMG) Information Assurance Standards 1 & 2 Information Risk Management for Information Communications Technology (ICT) systems
  - ISO 27000
  - ISO 27001 together with ISO 27005, COBIT 4.1 and CRAMM
  - UK Government Guidelines for public bodies, specifically HM Security Policies: Information Assurance Maturity Model
  - BS 31100 as the main risk management code of practice, elements of PRINCE2 for change, programme and project risk, and of the Risk Management Standard by Alarm and the Institute of Risk Management
  - the Australia and New Zealand Risk Management Standard and Companion 4360, 2004 (two organisations have adopted this methodology).[198]
  - Within the health sector, one NHS trust respondent has adopted several sector-specific risk management approaches: NHSLA Risk Management Standards for NHS Trusts providing Acute, Community, or Mental Health & Learning Disability Services; the Department of Health Integrated Governance Handbook, 2006; Department of Health,

[198] The ISO released its Risk Management Standard ISO 31000:2009 on 15 November 2009, four years after establishing a working party to develop the first international risk management standard using AS/NZS 4360:2004 as its working draft. This resulted in Standards Australia adopting the ISO 31000 as an Australian/New Zealand Standard and therefore making AS/NZS4360:2004 redundant. See http://sherq.org/31000.pdf.

Assurance: The Board Agenda, 2003; Department of Health, Building an Assurance Framework: A Practical Guide for NHS Boards, 2003.

- All of the respondents consider, or are in the process of considering, privacy risk as part of their overall risk management process, and therefore focus on "the wide range of risks to which the project/activity is potentially exposed", with privacy risk regarded as an element of risk exposure. In one organisation, privacy risk is already "a sub-category of the risk management assessment process", therefore locates PIA within existing assessment routines.
- All of the respondents have established close collaboration between the risk manager and the data protection officer regarding privacy risks, with the data protection officer working closely with the risk manager "on relevant issues, and providing updates to one another as to current guidance/awareness".

7.3 THE JANUARY 2013 SURVEY RE PIAS, PROJECT AND RISK MANAGEMENT

An important element in the present Trilateral study has been a survey of public and private sector entities to determine whether they undertake privacy impact assessments and which project and risk management methodologies they use. We undertook the survey to give us some actual empirical data and to give us a better idea of how easy or difficult it might be to better integrate the PIA process with existing project and risk management processes. The following pages provide some details of the findings from our survey, which was initiated in January 2013.

7.4 COMPILING CONTACTS FOR THE JANUARY 2013 SURVEY

Trilateral compiled an extensive list of contacts for the distribution of its questionnaire in January 2013. The list contains 829 contacts of both public and private stakeholders. Public organisations comprise central government bodies, NHS trusts and local authorities, while private organisation contacts include mainly FTSE100 and FTSE250 companies. In addition, the contact list also captures a small sample of private hospital contacts (50 contacts). In order to ensure representation across the different public sector categories, we identified and compiled contacts for several sub-categories of central government bodies, NHS trusts and local authorities. The central government category comprises all ministerial departments, non-ministerial departments, executive agencies, government-owned corporations and a random sample of non-departmental public bodies. The NHS trusts includes primary care trusts (PCT), acute trusts and foundation trusts, operating in the South East and London. Finally, local authorities include single, two-tier and sui generis authorities in England. For each organisation, we initially aimed at collecting two different contacts: the contact for the data protection officer and the risk manager. However, due to difficulties in finding specific contact information, this was not always possible. Table 7.1 shows the number of contacts for each sector of stakeholder that we were able to compile.

Sector	No. of contacts
Central government bodies	154
Local authorities in England	307
NHS trusts and private hospitals in England	268

Private companies	100
Total	**829**

Table 7.1: Trilateral contact list for the January 2013 survey

During the compilation of the contact list, which took some weeks, we experienced different degrees of difficulties and challenges in acquiring the contact information. The unwillingness of some organisations, above all private companies, to provide an e-mail contact for their data protection officer (or anyone) came as a surprise. In the following section, we have summarised our experience in collecting data protection contacts for the different sectors of stakeholders.

Government departments and non-departmental public bodies (NDPBs)

In terms of identifying data protection contacts for the government departments, compared to finding private sector contacts, for some departments, it was relatively easy to find contacts (i.e., a data protection officer, information rights team, freedom of information contacts). FOI is generally well signposted on government department websites, which makes it comparatively easier to find FOI contacts than data protection contacts.

For the non-departmental public bodies, we were able to identify e-mail IDs for data protection officers, information managers, and a few senior information risk officers. In cases where we didn't get this information, we identified FOI contacts, other senior management (e.g., the CEO) and the communication teams.

Many departments have information management policies online. However, often these pages are not well signposted and it takes a bit of searching to find them on the website. At other times, data protection contacts were embedded in the FOI policy section or could be found only after looking at the FOI section of the organisation's website. Many departments have common teams for data protection and FOI.

Though the White Book proved a useful resource, it does not mention data protection or freedom of information contacts.

Perhaps data protection contacts could be embedded in privacy policies for which most organisations already have a dedicated section.

Local authorities

The identification of a data protection officer contact was generally not problematic in the local authority (LA) segment. Some councils have joint FOI and/or data protection officers and the contact details for these were often easy to find through a search engine or directly from the homepage of the council's website. Data protection officer information was often displayed in relation to subject access requests, although many councils did not provide an e-mail or phone number on this page, as they request that subject access requests be made in writing to a postal address. The contact details for FOI or information governance officers could often be found on copies of replies to FOI requests on websites such as www.whatdotheyknow.com.

Determining which local authority officer held the senior information risk officer (SIRO) responsibility was harder, and sometimes required guesswork. These responsibilities were

found in heads of ICT, directors of legal, corporate services, resources, deputy chief executive and chief executive offices. Risk management was not generally regarded as a "public-facing services" so did not appear on lists of services, frequently asked questions or other similar guides to help people navigate LA websites.

An occasional problem arose where a local authority website (particularly for the larger authorities) had a very large amount of documentation available, but with a fairly basic search function, that returned little detail about the search results. Information and contacts could be buried under a volume of other documents.

There was significant variation amongst local authorities in the accessibility and transparency of contacts. Some councils published names, direct phone numbers, and e-mail addresses for a large number of employees, often down to heads of service, or managerial roles, whilst others provided only the heads of directorates, and without an e-mail or direct dial phone number. Some local authorities provided switchboard phone contacts for named individuals. Several councils use a "contact us" form on the webpage rather than providing an address. Once a name or job title had been identified, the council call centres were generally able to provide an e-mail address, although some were unwilling to provide a direct dial number, preferring to put a caller through to the contact.

Many council websites share a similar structure, and detail of the executive boards of a council can often be found under the "Council and Democracy" or "Your Council" sections of the websites. Local authority ICT strategies of recent dates were a productive source of contacts in ICT, information governance and risk management.

NHS Trusts

Finding data protection and SIRO contacts for primary care trusts (PCTs) was made difficult because of the reorganisation currently going on in the NHS. Since 2011, many PCTs have been merged into "clusters" that combine several PCTs, often sharing board members. These clusters sit below regional Strategic Health Authorities. Commissioning responsibilities are currently being devolved down to clinical commissioning groups as part of NHS reforms. These groups currently exist in a shadow role with the PCTs. It is often unclear where data protection decision-making is occurring and who the SIRO is. A single board member of a cluster may be the SIRO for several PCTs. Also, the clustering appears to have had a hollowing-out effect on PCT websites, with most of the local content being archived.

In general, PCTs are less transparent than local authorities. They provide names and biographies for board members but little detail about the management structures under these board members of their specific responsibilities. Few to no PCT websites provided easily accessible e-mail addresses or direct dial phone numbers for board members. PCT strategy and policy documents tended to be signed by officer holder roles (e.g., head of governance) rather than by named individual. Given the reorganisation into clusters, many of these documents were also out of date.

Each NHS organisation should have an appointed "Caldicott Guardian" with responsibilities for patient data protection.[199] This role was not easily obtainable from the websites of most

[199] According to the Department of Health, a Caldicott Guardian "is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing". http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott

PCTs. NHS Connecting for Health maintains a publically accessible register of Caldicott Guardians, but this register does not contain e-mail addresses or phone numbers.

For NHS foundation and acute trusts, we identified contacts such as data protection officers, information governance managers, FOI leads, senior information risk officers. For some organisations, it was easy to get the data (once one knew where one was looking), for others it took a bit of time. Again, FOI contacts are more easily found.

Private hospitals

Private hospitals appear to have centralised data protection, information governance and information security roles at the group and/or corporate level. Very little contact information was available on their websites. Switchboard and call centre staff were willing to connect to named members of staff, and sometimes to provide e-mail addresses, but not provide direct dial numbers. There was little information about privacy and data protection processes on these websites, other than the website privacy policy. Where data protection information was provided, there was rarely a specified contact, and queries were directed towards the generic "info@..." e-mail address. The names (although not e-mails and phone numbers of hospital managers) were available on some websites.

Companies

It was extremely difficult to compile the contacts for private companies. Very little contact information was available on their websites. Switchboard and call centre staff were often unwilling to connect to named members of staff or provide e-mail addresses. There was little information about privacy and data protection processes on company websites, other than the generic website privacy policy. Where there was data protection information provided, there was no specified contact provided, and queries were directed towards the generic "info@..." e-mail address. In addition, even if the website provided the company's annual report, this did not include any specific names and/or contacts and was often difficult to find. As a result of the lack of publicly available contact information, we were forced to initially rely on company information, provided by stock market websites, and then on social networking sites as well as Trilateral's own network of professional contacts. Overall, it was a surprise to experience the extent of information asymmetry that appears to characterise the relationship between the public and private companies. Undoubtedly, well signposted and publicly available contacts for the data protection officer, or similar figures within the company, could help start addressing this asymmetry.

7.5 RESULTS FROM THE JANUARY 2013 SURVEY

Following the ICO's award of the present contract, Trilateral sent an expanded questionnaire to FTSE 100 and FTSE 250 companies, central government departments and agencies, local authorities and NHS trusts in order to have a more accurate understanding of which risk management standards or methodologies are being used and how commonly privacy risks are included in their risk management practices. We sent the questionnaire to our internally developed contact list of 829 contacts. In addition, the Data Protection Forum, a non-profit association bringing together professionals to discuss data protection, freedom of information and related topics, distributed the questionnaire to its 250 members, from more than 120 public and private sector companies and organisations. The ICO also e-mailed a link to the

survey to 1,300 data protection officers who were either being offered a place at the ICO Data Protection Officer Conference or were on the waiting list. Finally, the IAPP Europe Data Protection Digest published a story on this study with a link to the survey via its online newsletter of 25 January 2013.[200] Overall, we expect that the survey should have reached more than 2,500 potential respondents.

See Annex 4 for the questionnaire.

The survey provides empirical evidence with regard to the extent to which organisations in the UK already follow risk assessment approaches that take privacy impact assessment into consideration and/or that could do so.

Table 7.2 shows response rates for the overall sample and for the key sectors of stakeholders included in the survey (i.e., central government bodies, NHS trusts, local authorities and private companies). We have also included a few responses from an unknown sector[201] and civil society organisations, including professional associations, which we collected during the ICO conference. Response rates have been calculated based on the overall size of the target populations since we assume that the survey should have reached all of the organisations within the target sectors. For the unknown sector and civil society organisations we do not have a target population, therefore we have reported only the number of responses received. Although we used several channels to reach respondents, the majority of the responses received were from the Trilateral contact list. We have received very few responses from the ICO, IAPP and Data Protection Forums contacts. We assume that one of the reasons why the response rates from the latter have been so tiny is that they sent their contacts the questionnaire in PDF form whereas we sent our questionnaire as a Word file. Probably it was much easier for respondents to respond to the Word file than the PDF file.

Category	No. of responses	Size of targeted population	Response rate
Unknown	12	NA	NA
Private Sector	12	350	3%
Civil Society	2	NA	NA
Central Government	25	372	7%
Local Authorities	62	432	14%
NHS Trusts	35	318	11%
Overall	**148**	**1472**	**10%**

Table 7.2: Response rates

[200] This was the item in the IAPP Europe Data Protection Digest of 25 Jan 2013:

DATA PROTECTION -- UK

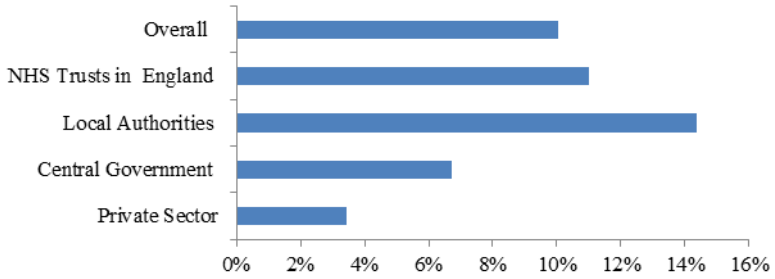
ICO Looks To Improve PIA-Risk Management Integration

In an attempt to improve integration between privacy impact assessments and existing project and risk management processes, UK Information Commissioner Christopher Graham has appointed Trilateral Research & Consulting to analyze the current landscape and produce a report highlighting practical guidelines for integration. The ICO is looking for public- and private-sector organisations to respond to six questions aimed at assisting with the project. Deadline for the questionnaire is slated for early February. **Full Story**

The IAPP subsequently informed us that they e-mailed the IAPP Europe Data Protection Digest to 4,935 members.

[201] We have allocated the category of "unknown" sector to completed questionnaires which we could not allocate to any sectors.

Figure 1: Response rates for targeted sectors



We also find it unfortunate that relatively few companies chose to respond to the questionnaire. Although many companies want to hoover up as much information about their customers as possible, they appear unwilling to reciprocate in even the smallest modicum – e.g., almost none provides the names or telephone numbers or e-mail addresses of their data protection officers. One can only assume that companies do not wish to be distracted from their profit-making activities by responding to requests about how they are using their customers' personal data. The information asymmetry here is striking. Even though much research shows that transparency helps to build trust, few companies seem interested. There are a few exceptions, however.

7.6 THE MOST POPULAR PROJECT AND RISK MANAGEMENT APPROACHES

In this section, we identify the project and risk management standards and methodologies used by respondents to the January 2013 survey and, in particular, which are the most popular based on the responses received.

As tables 7.3 and 7.4 indicate, the vast majority of the surveyed organisations follow some particular risk and project management methodologies and standards (86% and 90% respectively).

	1. Does your organisation follow a particular risk management methodology (e.g., ISO 29100, ISO 27000, ISO 31000)?	%
Yes	122	82
No	24	16
Don't know	0	0
Declined to answer	2	1

Table 7.3: Adaption of risk management methodologies and/or standards

	2. Does your organisation follow a particular project management methodology and/or standard (e.g., PMBOK, PRINCE2, etc.)?	%
Yes	133	90
No	11	7
Don't know	1	1
Declined to answer	3	2

Table 7.4: Adaption of project management methodologies and/or standards

Furthermore, of the organisations that have implemented particular project and risk management methodologies and /or standards, the majority follow one single project and risk management methodology and/or standard (see table 7.5). However, within the local government and NHS sectors, some organisations adopt more than one single risk management methodology and/or standard. Table 7.6 indicates that the average number of risk management methodologies and standards adopted in local government and NHS trusts is two, with a maximum of standards adopted by a single organisation being four in local government and 14 in NHS trusts. In relation to project management methodologies, civil society organisations appear to use an average of two project management standards.[202]

No. of methodologies/standards in use	No. of organisations	%
1 project management standard/methodology in use	108	81
1 risk management standard/methodology in use	77	63

Table 7.5: Utilisation of one single project and risk management methodology and/or standard

Sector	No. of organisations implementing PM	No. of organisations implementing RM	Average no. of PM in use	Min	Max	Average no. of RM in use	Min	Max
Unknown	10	8	1	1	2	1	1	2
Private sector	7	7	1	1	2	1	1	2
Civil society	1	1	2	2	2	1	1	1
Central government	23	23	1	1	3	2	1	3
Local authorities	58	52	1	1	3	2	1	4
NHS trusts	34	31	1	1	3	2	1	14
Overall	133	122						

Table 7.6: Average number of adopted PM and RM methodologies and/or standards

Tables 7.7 and 7.8 indicate which specific risk and project management methodologies and/or standards are the most popular, based on the responses received. In relation to risk, the family of ISO standards is the most adopted, with ISO31000 being the most popular (20% of the organisations, who have a risk management methodology, follow this standard). Bespoke and internally developed risk management frameworks are also popular (26% of the organisations, who have a risk management methodology, have their own internally developed risk

[202] Since the sample comprises only two civil society organisations, the findings for this sector are not sufficiently robust and should only be considered as indicative.

management framework). However, these internally developed risk frameworks are often used together with other sector specific, recognised standards (i.e., STORM or NHS guidances) or they are partially based on the ISO family of standards.[203]

Risk management methodologies and standards	No. of organisations using the standard	%
Its own risk management framework	28	23
ISO31000	24	20
ISO27001	15	12
ISO27000	15	12
M-o-R management of risk by Office of Government Commerce	11	9
Treasury's Orange Book	11	9
Risk Management Standards by Alarm, the Institute of Risk Management and the Association of Insurance and Risk Managers	10	8
NHS Information Governance Toolkit	8	7
AS/NZS 4360	7	6
National Patient Safety Agency Guidance	5	4
CIPFA/Solance Framework for Corporate Governance	4	3
ISO27002	3	2
HMG Security Policy Framework	3	2
HMG Information Assurance Standard No.1, (IS1)	3	2
NHSLA Risk Management Standards for NHS Trusts providing Acute, Community, or Mental Health & Learning Disability Services	3	2
ISO27005	2	2
BS 31100:2008 Risk management	2	2
HMG Information Assurance Standard No 2: Risk Management and Accreditation of Information Systems (IS2)	2	2
HSG 65 method	2	2
Department of Health, Integrated Governance Handbook, 2006	2	2
NHS Litigation Authority Risk Management Standards	2	2
STORM by Zurich Municipal Management	2	2
ISO9001	1	1
BS 31100:2009 Risk management	1	1
BS 31100:2011 Risk management	1	1
Managing Information Risk, 2008, by National Archives	1	1
COBIT 4.1	1	1
CRAMM	1	1
AS/NZS ISO 31000:2009	1	1
HMG Information Assurance Maturity Model	1	1
Home Office Risk Management Policy	1	1
UK's Data Protection Act 1998 (DPA)	1	1
HMG IA Standard No 6	1	1
RMADS	1	1

[203] Of the 21 organisations using their own, internally developed risk management frameworks, five organisations (24 % of this group) also adopt another risk management standard (i.e., ISO family or NHS guidance), while four organisations (19 % of this group) have partially based their own risk framework on one standard of the ISO family.

Risk management methodologies and standards	No. of organisations using the standard	%
JCAD RISK system	1	1
Department of Health, Building An Assurance Framework. A Practical Guide for NHS Boards, 2003	1	1
Making a Difference – Review of Controls Assurance Gateway Ref. No. 4222	1	1
Governing the NHS: A guide for NHS Boards (2003)	1	1
Intelligent Commissioning Board (2006 & 2009)	1	1
The Healthy NHS Board: Principles for Good Governance (2010)	1	1
Taking it on Trust – Audit Commission (2009)	1	1
Health and Safety at Work Act 1974	1	1
Care Quality Commissioning Compliance Toolkit	1	1

Table 7.7: Most popular risk management methodologies and/or standards

In relation to project management methodologies and standards, the majority of the surveyed organisations, 85%, follow PRINCE2 (113 of the organisations with a project management methodology in place use this standard). Internally developed project management frameworks follow, with 21 of the organisations who use project management methodologies, which is equivalent to 16%, having their own bespoke framework. As in the case of internally developed risk management frameworks, these internal approaches are often used together with, or are partially based on, other recognised project management standards (e.g., PRINCE2).[204]

Risk management methodologies and standards	No. of organisations using the standard	%
PRINCE2	113	85
Its own project management framework	21	16
Agile/DSDM	5	4
MSP (managing successful programmes)	5	4
PROMPT2 by APM	1	1
P30	1	1
PM Connect tools	1	1
Lean 6SIGMA (DECODER)	1	1
PMP (Project management professional)	1	1
P3M	1	1
National Computing Centre guidelines	1	1
Capital Investment Manual	1	1

Table 7.8: Most popular project management methodologies and/or standards

[204] Of the 16 organisations following their own bespoke project management framework, five of them (31%) have also adopted PRINCE2, while four (25%) have partially based their own framework on PRINCE2.

7.7 OTHER FINDINGS FROM THE SURVEY

The survey responses also provide interesting insights in relation to the adoption of PIA and its integration into organisations' risk and project management processes.

Based on the responses received, the majority of the surveyed organisations take into account privacy risks in the context of their overall risk and/or project management processes (83%), while 76% (113) have established collaboration between the risk manager and data protection officer in relation to privacy risk, and 68% (100) perform PIA (see tables 7.9, 7.10 and 7.11).

	3. Does your organisation currently take account of privacy risks in the context of its overall risk and/or project management process?	%
Yes	123	83
No	12	8
Sometimes	6	4
Considering	3	2
Don't know	1	1
Declined to answer	3	2

Table 7.9: Integration of privacy risk

	6. Is there any collaboration between the risk manager and the DPO regarding privacy risk management?	%
Yes	113	76
No	12	8
Sometimes	12	8
Considering	3	2
Don't know	4	3
Declined to answer	2	2%
NA	2	1

Table 7.10: Collaboration between the risk manager and DPO

	4.a Does your organisation perform privacy impact assessment?	%
Yes	100	68
No	38	26
If required	4	3
Don't know	4	3
Declined to answer	2	1

Table 7.11: Adoption of PIA

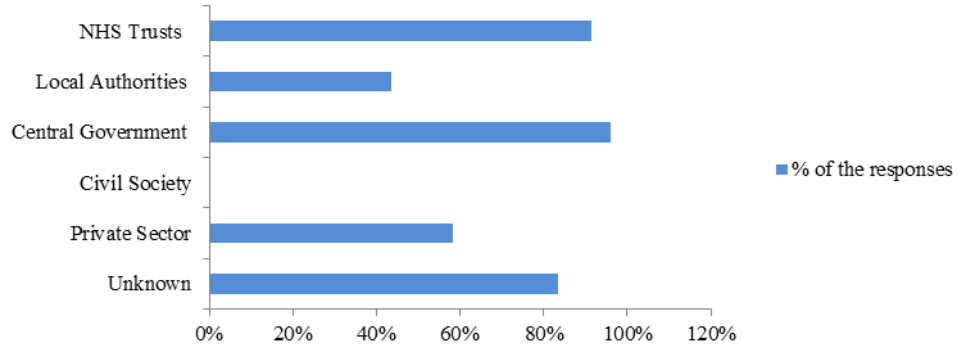
In relation to specific sectors, central government has the highest number of organisations performing PIAs (96%), followed by NHS trusts (91%). Civil society organisations and local

authorities have the lowest number of organisations performing PIAs, 0% and 44% respectively. Within local authorities, the same percentage of the sample, 44%, do not perform PIAs at all (see table 7.12).

Sector	No. of organisations performing PIAs	% of the sector responses	No. of organisations not performing PIAs	% of sector responses
Unknown	10	83	2	17
Private Sector	7	58	3	25
Civil Society	0	0	2	100
Central Government	24	96	1	4
Local Authorities	27	44	27	44
NHS Trusts	32	91	3	9
Total	100		38	

Table 7.12: Sector adoption of PIA

Figure 2: Percentage of organisations doing PIA by sector



The reasons for not performing PIAs range from the practical need of not having in place "more resources" and experiencing problems with "obtaining buy-in from Project Management Staff (particularly where they are new to the organisation)" to more fundamental barriers related to the PIA processes being "too onerous in their current form". The former barrier is more prevalent within local government organisations, while the latter has been voiced by the private sector. In addition, cultural obstacles still appear to play a part in relation to the use of PIA, with a few organisations believing that PIA "is not considered to be necessary as data protection rules are strictly followed throughout the organisation".

However, these results represent the minority of our respondents. As shown in tables 7.11 and 7.12, the majority of the organisations surveyed do undertake PIA with several organisations, above all local councils, in the process of "introducing", "piloting" or "incorporating PIAs", "starting with procurement and commissioning exercises" but also "as part of formal project documentation" and project management procedures. From the majority of the comments that the respondents wrote in the questionnaire, the reader could infer that these more formal integration attempts have only just started and that, at present, several of the organisations undertaking PIAs still do so on an ad-hoc basis: "PIAs are conducted on an ad hoc basis where particularly relevant." Furthermore, irrespective of the perceived present barriers to performing PIAs, the majority of respondents believe that PIA can be integrated

into the existing organisational risk procedures. Indeed, as table 7.13 shows, the majority of the organisations that do not perform PIA do think that it would be possible to introduce PIA as part of their risk management process (30 of the 38 organisations that do not perform PIA believe that it would be possible to include PIA in their risk management processes).

	5. If you do not do PIA, do you think it would be possible to include PIA as part of your risk management process?	%
Yes	30	79
No	2	5
If required	3	8
Maybe	1	3
Don't know	2	5

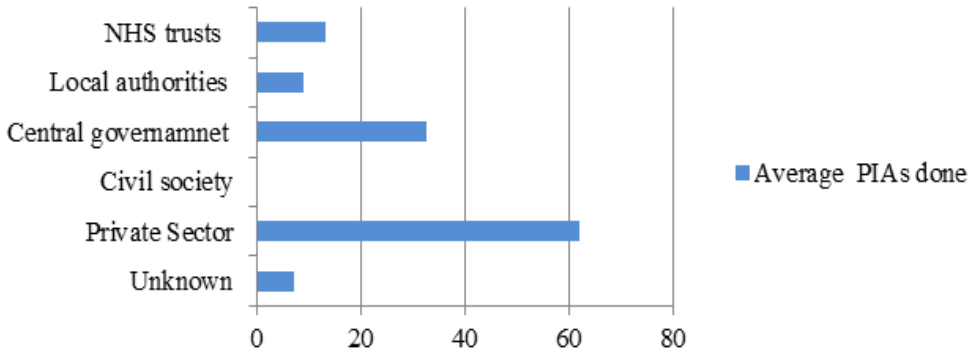
Table 7.13: Possible integration of PIA into risk management process

In relation to the number of PIAs done by the organisations that perform PIAs, the private sector has the highest average of PIAs undertaken, 62, followed by central government, 33, NHS trusts, 13 and local authorities, 9 (see table 7.14 and figure 7.3). In addition, irrespective of the sector, some organisations, 15, equivalent to 15% of those organisations performing PIAs, could not say how many PIAs they have done since they do not have a centralised repository for PIAs and this information is not recorded. See Annex 5 for more details on the number of PIAs done by individual respondents.

Sector	No. of organisations performing PIA	Average no. of PIAs done	Max no. of PIAs	Min no. of PIAs
Unknown	10	7	43	2
Private sector	7	62	400	1
Civil society	0	0	0	0
Central government	24	33	500	0
Local authorities	27	9	178	0
NHS trusts	32	13	186	0
Total	100			

Table 7.14: Number of PIAs done by sectors

Figure 3: Average number of PIAs done by sector



The respondents surveyed also commented on the ICO's PIA Handbook. Although several organisations claimed that they use the ICO PIA guidelines, the majority appear to have adapted the PIA process and assessment, suggested by the ICO, and developed a more simplified and tailored approach for doing PIA. Listed below are some of the more negative comments that some of the respondents made in relation to the ICO's PIA guidelines. While these should be viewed as a minority, most of the comments, whether positive or negative, underline the need for a more simplified and sector-tailored PIA approach.

Respondents' comments on ICO's PIA guidelines and Handbook

- "... from our experiences to date it is clear that the PIA process as advised by the ICO is overly cumbersome and should be limited to being seen as a control measure within an overall Information Risk Assessment/Mitigation process and not a standalone measure."
- "We are aware of the ICO PIA process; however, the Trust follows a more simplified agreed local process. This process is followed in all relevant IM&T projects and system implementations."
- We do PIAs but "we do not use the ICO's format which is too long and inflexible."
- "The problem is the length of the formal PIA provided by the ICO. It is easier to have our own checklist which is more simplistic."
- PIA could be introduced "If there was a version that could be developed for health which was easy to use and supported by Department of Health or with the NHS Information Governance Toolkit."
- "From experience, PIAs are sometimes not simply the best for risk management. In such circumstances, we have used the data compliance checklist list where already existing IT systems are reconfigured to process new personal data."
- PIAs cannot be integrated as "presently operated. PIAs may be appropriate for new or changing services but there is no centralised procedure for these. Changes are usually incremental, or services are adopted from existing providers, so that it is not at all clear that PIAs are useful or helpful, or that risks have increased through not applying them.

8 ANNEX 3 – CASE STUDIES

This annex deals with a selection of key case studies of public and private sector entities that were also part of the survey. The case studies are based on interviews that we conducted with selected respondents to our questionnaire. We have used the case studies to further investigate how organisations have practically integrated privacy impact assessment into their existing project and risk management methodologies and processes, as well as identify key lessons learned from their experience of the integration and the use of the ICO PIA Handbook.

Partly to compensate for the low response rate to the survey from private companies, we selected several case studies from within the private sector.

In the case studies, we also indicate whether the organisations have any "open doors", i.e., any points in its project and/or risk management processes where a PIA could be inserted and carried out and, if so, where are those open doors, at what point in the project and risk management process could a PIA be introduced.

Case studies 9 – 12 are different from the first eight case studies. Case studies 9 – 12 focus particularly on where or when government departments take privacy and PIAs into account in the policy-making process.

8.1 CASES STUDIES: EXPERIENCE WITH PIA AND THE ICO HANDBOOK

8.1.1 Case study 1: A global company

Organisation's description

The company, headquartered in London, operates in more than 80 countries. It has a primary listing on the London Stock Exchange and a secondary listing on the New York Stock Exchange. It is a constituent of the FTSE 100 Index and has market capitalisation of more than £80 billion (as of July 2012). Since 2001, the company has had a global data protection and privacy policy, articulating global standards with respect to data privacy compliance. Recently, the company's privacy policy has been replaced by specific data privacy rules, which communicate the standards contained within the privacy policy by expressing them in the form of rules ("the rules"). The rules, together with internal practical procedures and principles, all based on European data protection standards, constitute a binding corporate governance framework. The rules must be followed by each employee and contractor when handling personal information. Applying European data protection standards across the company's global network by means of "the rules" has been found the best way to ensure that an adequate level of protection exists for transfers of personal information across the company's international operations.

Experience with the integration of privacy impact assessment

This company uses its own bespoke project and risk management methodology. As stressed in the company's response to the questionnaire, integration has been achieved at the project initiation via an internal, online information security assessment, which includes privacy risk

in the form of data protection risk: "All projects have to go through a digital security and privacy assessment (PIA)." The project manager, who is assigned to a project, has the responsibility to complete a security assessment online for the project. The tool has a simple question in relation to privacy risks: "Does your project involve personal data?". If the project manager answers "yes" to this question, then he or she is required by the company's internal processes to do a privacy impact assessment (PIA), which the privacy team has designed to meet the company's own requirements. The PIA is then sent to a central PIA repository and to the privacy team, which comprises four people focusing on four global regions. The privacy officer, responsible for the global region, where the project is going to be implemented, will go through the PIA and contact the project manager to provide all the information needed in relation to the region's privacy requirements and discuss these requirements in detail to properly identify, assess and manage potential impacts. The project manager will then prepare a briefing paper in relation to how the project will meet the privacy requirements together with further questions for the privacy team if there any doubts on how to achieve full compliance. The privacy team will finalise the privacy requirements and mitigating actions, which will be implemented during the project life cycle.

In addition, for large projects, the company could appoint a privacy manager, who is in charge of managing the privacy assessment process, making sure that all the documents are completed and returned from the different offices, and delivering the agreed mitigating actions within the project.

Integration of privacy risk, in the form of data protection risk, into the company's existing risk processes is also achieved via the procurement stage, before project initiation, when the privacy team could get involved in assessing procurement orders and providing privacy advice.

	"Open doors" for privacy impact assessment integration	**Explanation**
1	Pre-project: procurement stage	During the procurement stage, the privacy team assesses procurement orders and provides privacy advice. The company has not fully formalised this process.
2	Project initiation: Information security assessment	The focus is to perform an online information security assessment, which includes privacy risks in the form of data protection risk. This will trigger a PIA process if the project manager identifies privacy as a potential risk.
3	Project implementation: Privacy work stream	All large-scale projects might have a formal privacy work stream designed to manage the company's privacy processes and monitor implementation of agreed mitigating actions as the project progresses.

Experience with the ICO PIA guidelines

The privacy team looked at the ICO PIA guidelines but found that these did not meet company's requirements. Therefore, the team developed its own PIA process. The respondent identified as key barriers for implementing the ICO PIA guidelines: the number of questions

that the project manager needs to answer in the initial assessment phase, when organisations determine if a PIA is needed, and the complexity of the privacy risk assessment process suggested in the ICO Handbook. The company found that the initial screening questions were too many. This is because project managers must already complete a very detailed digital information security questionnaire. In order to address these barriers, the company has developed a very easy initial assessment (e.g., one question) and a light and high level PIA, which the project manager can easily complete (i.e., the average time to complete a PIA is about two or three days). This ensures full uptake of the privacy process by project managers and a good stepping stone for the more detailed assessment, which is done together with the privacy team, when follow-up questions and discussions of specific requirements are aligned and adapted to the specifics of the project and the region where the project is going to be implemented. As stressed by the respondent, the company's strategy has been to try to "keep the PIA as simple as possible, while extracting the minimum amount of information at the beginning of the process" and then "become more detailed and specific" with the follow-up process, when questions are discussed and specific requirements and mitigating actions agreed between the project manager and the privacy team. Overall, the respondent feels that the ICO PIA Handbook is "not business friendly" but rather "too onerous and detailed". Indeed, the respondent suggested that the ICO should do some consultations with representatives of different sectors to decide what should be adapted and removed from the guidelines and how the guidelines can be better integrated with "the working of the business".

.

	Identified barriers to the use of ICO PIA guidelines	**Respondent's recommendations for improving the ICO PIA guidelines**
1	Too many initial pre-assessment questions	Set up consultations with different industry sectors to integrate the sector view and practical experience into the guidelines.
2	Guidelines are not business friendly	Better integrate the guidelines with the "working of the business".
3	Guidelines are too detailed and onerous	Simplify and shorten the PIA Handbook.

Key lessons learned

The company shared with us a few lessons learned from its practical experience of integrating privacy risk into its existing risk and project management methodologies and processes.

First, from a global point of view, it is useful to categorise all the countries where the company operates into risk areas based on the privacy risk of compliance. This categorisation has helped direct the company's focus and resources, and to effectively engage with a global network of offices across the company's international operations.

Second, the documentation that the privacy team provides to support project managers when they do the PIA is important. Project managers must have all the information and the questions and answers they need to do a proper assessment. It is important to give them all the necessary data they need to allow them to make the necessary project adjustments in order to be fully compliant.

Third, PIA should be approached as a triage process, where priorities and interventions are determined based on the severity of the situation. If the situation is not serious, project managers and privacy teams should not need to complete too many forms and answer too

many questions. Conversely, if the situation is serious, both project managers and privacy teams need to perform in-depth and tailored assessments.

Fourth, privacy teams should establish relationships with other business functions, for instance, via an internal data privacy network, to support and reinforce the company's privacy culture.

Key motivations for integration

Within the company, the key motivation for achieving effective integration between privacy risk and project and risk management processes originates from the company's code of conduct, "the rules", and the adopted governance framework. Both of them take data privacy compliance very seriously, according to our respondent.

8.1.2 Case study 2: A life assurance company

Organisation's description

The company has grown from a small local business to one of the UK's financially strongest life assurance companies with industry-wide recognition, while still preserving its mutual status. With more than £4 billion of assets under management, this mutual provides tailored financial advice and services to select professional customers, such as doctors, dentists, teachers and lawyers. Despite the faltering economy, the company has enjoyed a period of sustained economic growth in recent years with new business sales having increased by more than 50 per cent from 2008 to 2011. Based on an independent survey, its customers also appear to value its products and services with more than 85 per cent of them saying that the mutual "really cares about them".

The company collects and stores personal data about its customers, which it uses for the provision of products, services, administration, marketing, risk assessment, fraud prevention and regulatory purposes. It may also need to disclose this information to other service providers or carefully selected third parties for these purposes. In addition, the company uses cookies to gather additional data about customers' behaviour and may include web beacons (also known as clear GIFs or web bugs) in its e-mails to customers to track the success of its marketing campaigns. Customers can, however, opt out of the cookies and marketing campaigns by following web-based instructions for deleting existing cookies and disabling future cookies and web beacons. The mutual does not have a dedicated data protection officer but instead the company's risk manager is also responsible for privacy risks. We found no evidence – through the questionnaire, interview and desktop analysis – that the company has developed and implemented a strong privacy policy and governance framework.

Experience with the integration of privacy impact assessment

This company uses its own bespoke project and risk management approach. As stressed by the respondent, both approaches are "quite detailed" and designed to closely meet the company's needs and specific requirements. Privacy risk is not formally integrated into the company's existing project and risk management processes and, as stressed in the company's response to the questionnaire, the company takes privacy risks into account only occasionally. This normally happens on an ad hoc basis when the project manager decides autonomously to

go and see the risk manager if he or she believes that there could be some privacy risk involved in his or her assigned projects. At this stage, the risk manager, together with the project manager, will decide, by applying the ICO guidelines, if a PIA, and what type of PIA, is required. So far the company has never determined that a PIA was needed. Furthermore, the risk manager could provide no indication of the number of times project managers have contacted him about potential privacy risks.

	"Open doors" for privacy impact assessment integration	Explanation
1	Project initiation: ad hoc requests	The company has not implemented a proper, formal integration. Project managers are left on their own to decide whether their projects might involve privacy risks.

Experience with the ICO PIA guidelines

The respondent was quite critical about the PIA Handbook and identified several barriers for implementing the ICO PIA guidelines: the number of questions that the project manager needs to answer in the initial assessment phase, when organisations determine if a PIA is needed (i.e., there are too many questions), the ICO Handbook's poor alignment to risk assessment approaches, tools and documentations, and the interpretative and high-level nature of the ICO guidelines. Overall, the respondent feels that the ICO Handbook has been "badly conceived and executed". The Handbook's focus is too much on providing "check lists" rather than tackling the "issues that companies need to address". The respondent's preference is having a Handbook that is both principle-based and practically focused, ideally offering companies a risk assessment approach and practical risk tools that can be easily implemented. His view on the ICO recommended PIA is that it is "too onerous in its current form"; instead it should be "easy to use and provide beneficial outcomes".

	Identified barriers to use of the ICO PIA guidelines	Respondent's recommendations for improving the ICO PIA guidelines
1	Too many initial pre-assessment questions	Principle-based but also practical
2	The guidelines are too onerous	Easy to use and providing business benefits
3	The guidelines are too general	Simplify and shorten the PIA Handbook
4	They can be interpreted in opposite and different ways	Less "check list" and "more problem solving", ideally providing practical risk assessment tools and approaches

Key lessons learned

Given that the company has not done a PIA yet, the respondent identified only one lesson learned from his experience with the integration of privacy risks into the company's existing processes. Critical for the integration is to define a PIA process that is easy and fast to implement.

Key motivations for integration

For the respondent, the key motivation to use PIAs should be driven by the fact that companies find PIAs easy to implement and beneficial for business outcomes. If this is not

the case, the only way to enforce use of PIAs within industry would be to make them a statutory requirement.

8.1.3 Case study 3: A global life insurance company

Organisation description

The company, with its head office in North America, is a global group that operates in 24 countries and serves millions of customers worldwide. It is an internationally diversified financial services organisation, providing retirement and pension products to individuals and groups through its operations in Canada, the United States, the United Kingdom and Asia. Its services focus on providing customers with innovative and flexible retirement solutions both directly and through financial advisers nationwide. In the UK, the company manages £12 billion of assets.

The company has adopted a global privacy framework and standards to ensure that an adequate level of protection exists for the privacy of its customer data. The company is committed to protecting the privacy of all personal information provided to them, while viewing the proper use of this information as the root of its success. On its website, the company stresses that its privacy commitment is more than complying with applicable country privacy laws but rather doing the right thing for the millions of its customers whose personal information might have been collected or received by the company. Strong privacy principles are at the core of the company's global privacy standards and reflect the company's commitments to safeguarding personal information in its care.

Experience with the integration of privacy impact assessment

In relation to project management approaches, the company follows PRINCE2. In relation to risk management, the company has its own bespoke framework, which differs for different parts of the business, as well as a suite of consolidated risk management policies and standards (around 20-30 in total) at the global group level, which the entire company needs to follow. Each group risk and compliance owner is responsible for reviewing and improving the global suite of policies and standards via an annual questionnaire, designed to assess whether the policies and standards are working and full compliance has been achieved.

Privacy is an important consideration for the company and, as a result, privacy risks are part of the global suite of consolidated risk management in the form of global privacy standards. The company has also implemented a global privacy governance framework. It has a global owner for privacy risks, the chief privacy officer, and regional privacy business owners, who report to the chief privacy officer, and are responsible for deciding how to implement the company's global privacy standards in their business region, while facilitating privacy compliance within the business. The chief privacy officer and all of the regional privacy business owners meet quarterly to discuss integrated planning on privacy and issues arising from the implementation of the standards. However, the regional privacy business owners are not the only ones responsible for ensuring compliance with the company's global privacy standards. The company has also allocated responsibility for privacy compliance within the

operating management structure.[205] Furthermore, internal requirements, and therefore the company's global privacy standards, must also be followed by outsourced service providers, used by the company to deliver its services.

At present, the company is introducing a formal process to ensure greater compliance with its global privacy standards, which require doing PIA for any new initiatives, including new proposals and any significant changes in the company's business processes (i.e., PIAs are mandatory within the company). The importance of security and privacy is constantly stressed, via internal communications, by both the regional privacy business owners and information teams. However, the respondent underlined that the company felt that a formal process was needed in order to ensure a consistent approach within the company and full compliance from all project managers. This formal process will be initially driven by a preliminary privacy assessment asking three simple questions: first, whether personal information is involved in a new initiative; second, whether personal information will be processed outside the country responsible for implementing the initiative; and third, whether the new initiative involves consent from customers.

At the project initiation, project managers complete a preliminary assessment, which will then be reviewed by the regional privacy business owner. If the project manager answers "yes" to any one of the three questions, he or she will need to complete a PIA in the form of a questionnaire. As underlined by the respondent, "this internally designed questionnaire, which meets closely the company's needs, provides a company-wide template integrating all of the compliance and risk requirements for any new initiatives". The PIA questionnaire has been colour coded to facilitate easy identification of potential compliance gaps by the project manager and comprises several sections, ranging from scope to accountability and safeguards. Project managers will apply the company's risk approach when completing the questionnaire and identify mitigation actions as appropriate. An internally developed guidance on how to complete the PIA questionnaire and PIA training will be provided to the project managers by the privacy business owner in each region. The company intends to localise the questionnaire for each business region. Once the project manager has completed the full questionnaire, it will be signed off by the privacy business owner and the security manager. The leadership team will then have the final saying on the level of acceptability of the identified risks and appropriateness of the proposed mitigating actions. The business privacy owner is also planning to include a "line", called privacy, similar to a project task, in each project plan template.

	"Open doors" for privacy impact assessment integration	**Explanation**
1	Project initiation: A preliminary privacy risk assessment	The focus is to perform an easy preliminary privacy risk assessment at the start of each project based on three simple questions. This will trigger a full PIA assessment if the project manager answers "yes" to any of the questions.
2	Project implementation: A privacy task in project plan	Each project plan will have a task, called privacy. This will ensure full visibility and monitoring for privacy risks.

[205] Therefore, for instance, if a new business procedure, involving personal data, is implemented in the company call centres, the head of the call centre is responsible for ensuring full compliance with the company's privacy standards.

	"Open doors" for privacy impact assessment integration	Explanation
3	Corporate level: Incorporation of privacy risks into the company's global suite of corporate policies and standards	Privacy risks are part of the company's global suite of policies and standards and as such are enforced as part of mandatory internal risk requirements.

Experience with the ICO PIA guidelines

Although the respondent found the ICO's two-page overview on PIA quite useful,[206] he did not use the ICO Handbook when devising the company's initial preliminary privacy assessment and full questionnaire. He said this was because the company needed a much more comprehensive and tailored PIA approach than the one provided by the ICO guidelines. The respondent found the guidelines to be "too high level" and general to serve his company's objectives. However, the respondent also stressed that he will reconcile the company's full privacy questionnaire with the ICO guidelines to be sure that the ICO recommendations are fully reflected in the company's PIA process.

Ideally, the respondent would like the ICO to provide guidelines that he can use to improve the company's existing tools on privacy. In addition, he pointed out that the ICO guidelines should make much clearer that PIAs are not only required for projects. Anything involving privacy and changes in the way in which companies operate, such as changes in internal policies and procedures, should require a PIA. The respondent expressed also an interest in knowing how his company benchmarks on privacy compared to others.

	Identified barriers to the use of ICO PIA Handbook	Respondent's recommendations for improving the ICO PIA guidelines
1	Too many initial pre-assessment questions	Fewer and tailored pre-assessment questions and simpler process
2	PIA guidelines are too high level and general	Guidelines should help businesses to improve their privacy tools
3	Handbook too focused on required PIA for projects	Make clearer in the Handbook that PIAs are not only required for projects but also for any changes that affect how the company operates.

Key lessons learned

The respondent had a few key lessons learned from his practical experience of integrating privacy impact assessment into the company's existing risk and project management methodologies and processes. First, all project plans should have a "line" called privacy, similar to a project task. This will ensure that all of the privacy requirements are fully visible to and updated and monitored by project managers. Second, project managers need additional training and clear internal guidelines on how to do PIAs and complete PIA forms. Third, companies should review annually both their PIA documentation and processes.

206

http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/PRIVACY_IMPACT_ASSESSMENT_OVERVIEW.ashx

Key motivations for integration

For the company, the key motivations for undertaking PIAs and integrating more formally privacy risks into the organisation's standard processes lie in its privacy commitment towards its customers (i.e., the company will look after customer data) and in the fact that PIAs make good business practice.

8.1.4 Case study 4: Large support service company with strong UK presence

Organisation's description

The company is a sales, marketing, distribution and business support services group. The group is organised and managed in five separate divisions: Energy, IT communication and home entertainment products, healthcare, environment, and food and beverage. The group currently employs about 10,000 people and is listed on the Irish and London stock exchanges. In recent years, the company's strategy has been to grow a sustainable, diversified business by concentrating on those activities where it has established, or has the opportunity to establish, leadership positions in its chosen markets. At present, the company has a market capitalisation of more than €2 billion and operates in 13 countries, with more than half of its profits generated within the UK.

The company has a very basic and high-level data protection policy to safeguard customer data and privacy. It does not routinely collect any information about individuals, except where it is specifically and knowingly provided by them. The company might use the collected customer data to send its customers information they have requested and to provide information that may be useful to them. The company informs customers of their right to opt out of receiving this information at any time. In addition, the company may share non-personal, aggregated statistical data about its site visitors' traffic patterns with partners or other parties. However, as stated on its website, it does not sell or share any information about individual users.

Experience with the integration of privacy impact assessment

This company uses its own bespoke and detailed project and risk management methodologies and standards, which vary for the different divisions of the business. As stressed in the company's response to the questionnaire, the company considers privacy risks as part of the company's overall compliance process by integrating privacy risks into the corporate risk register. However, the company does not have a formal PIA process in place and has only started to undertake PIAs. Privacy risks are, therefore, considered on an ad hoc basis. As underlined by the respondent, this is due to a previous lack of privacy sophistication and maturity within the business. The company has, however, realised that there are potential gaps and opportunities for improvements in the way it implements privacy compliance. As a result, the company has recently appointed a head of compliance in charge of reviewing the existing privacy policies and procedures, redeveloping the company's privacy policy and setting up new privacy processes, which will involve a formal PIA process. In addition, the company has also assigned the responsibilities for data protection and the role of data protection officer to the head of marketing in order to stress both the importance of data protection activities and their closer connection with the way the company deals with its customers.

In relation to the new formal PIA process, which the company will implement in the near future, the respondent's intention is to set up "a very slimmed down and simplified PIA procedure", formally integrated into the company's project management process. This will be characterised by a very simple, initial privacy assessment, based on whether new projects involve any use and/or development of "communication systems". If this is the case, the project manager, responsible for the project, will be required to do a mini PIA together with the data protection officer. Ideally, the mini PIA should not take more than a couple of hours for preparation, analysis and completion. The head of compliance is also designing internal privacy and PIA training to support the development of a privacy culture and PIA skills within the company. All of the completed PIAs will be then signed off by the data protection officer and head of compliance.

	"Open doors" for privacy impact assessment integration	**Explanation**
1	Corporate level: incorporation of privacy risks into corporate risk registers and compliance policies	Privacy risks are incorporated into the corporate risk register and the company's internal compliance policies.
2	Project initiation: simple, initial privacy assessment	The focus is for the project manager to perform a very simple initial privacy assessment, based on whether any new projects involve the use and/or development of "communication systems". If this is the case, a mini PIA needs to be done by the project manager together with the data protection officer.

Experience with the ICO PIA guidelines

The respondent indicated that he is using the ICO guidelines and PIA Handbook to develop the new PIA process. However, he stressed that he is "both slimming and simplifying" the process, and from the Handbook, taking only the "skeleton and what is relevant to the company". He emphasised that the PIA process needs to be "workable". Ideally the PIA should be a "two-page document in the form of an easy and fast checklist". Indeed, he has noticed that the ICO has started providing more simplified information and guidance, which is very useful to support adoption and implementation of the guidelines in a business environment. Finally, he indicated that an ICO Handbook providing more practical tools and guidance on how to assess privacy risks would also be valuable since businesses do not often have the knowledge and experience required to assess privacy risks.

	Identified barriers to the use of ICO PIA guidelines	**Respondent's recommendations for improving the ICO PIA guidelines**
1	Too many initial pre-assessment questions and complex PIA check list	Focus on a "workable" PIA process and a two-page PIA in the form of an easy and fast checklist
2	Guidelines are too complex	Simplify and shorten the PIA Handbook with greater emphasis on practical guidance and/or tools on how to assess privacy risks.

Key lessons learned

The respondent shared with us a few lessons learned from his own experience of integrating privacy risk into risk and project management methodologies and processes in different companies. First, it is important to gain the buy-in from the most senior people within the company. Second, PIA processes need to be connected with the development of privacy awareness and culture within the company. Companies need to devise effective communication and training strategies to sustain a change in the mindsets of, and the development of new skills for, project managers. Third, simplicity is the key to achieve full implementation and adoption of internal PIA guidelines and processes by all relevant employees within a business environment. Fourth, it is important to make clear to the business why and how privacy and PIAs are commercially relevant (e.g., if you do not adopt these privacy processes, the company risks corrupting and/or losing its customer data, which is a major business asset).

Key motivations for integration

Within the company, the awareness that privacy is closely connected to the wealth and health of the company's customer base as well as the realisation that customer data is an important business asset are the key motivations for achieving effective integration between privacy risk and project and risk management processes.

8.1.5 Case study 5: Non-departmental public body in health

Organisation's description

The organisation is an executive, non-departmental, public body (NDPB), operating under the Department of Health. This public body has its own internal data protection policy and code of practice on confidential and personal information, which is based on the Data Protection Act 1998 and is part of the organisation's overall information governance policy. The code of practice requires that all of the organisation's employees and suppliers take into consideration privacy impact as part of all decisions, involving the use of confidential personal data, such as collecting, using and/or sharing confidential data. This public body will only collect personal information volunteered by citizens, such as feedback from surveys and online forms, e-mail addresses and preferred means of communication. Furthermore, personal information will be only used to exercise the public body's functions, and to improve the quality and safety of its services. The information rights manager and the information security manager equally share responsibilities for data protection within the organisation. The organisation does not have a central database or repository for PIAs. As a result, the information rights manager could not estimate the number of PIAs so far undertaken.

Experience with the integration of privacy impact assessment

The organisation uses PRINCE2 as its main project management methodology, as it facilitates better control of resources and the management of business and project risks. For risk management, this public body has its own internally designed risk management processes, which are based upon industry best practices but do not follow any particular risk management methodologies and/or standards. As stated in the organisation's response to the questionnaire, "Privacy and risk to privacy is a core consideration within all our projects, and

they are managed accordingly. Privacy risks – mainly relating to information risk – have been identified and are managed within our overall risk management processes." The information rights manager has only very recently designed the internal process, integrating more formally privacy impact assessment into its existing project and risk management procedures. This more formal approach was considered to be necessary after, as stated by the respondent, "the organisation found that some projects that should have been considered for a privacy assessment were not." The new process is aligned with the ICO guidelines and triggered at the project initiation phase. At the start of a project, project managers need to complete a privacy assessment form for their assigned projects, which is based on 10 questions presented in the form of a risk assessment. The risk assessment form mainly focuses on privacy risks within information risks, with only some considerations related to personal privacy. All of the completed forms will then need to go for approval to the organisation's information governance corporate group,[207] who will assess the risks in more detail and provide specific guidelines for the project managers to follow (i.e., need for a small-scale PIA or full-scale PIA or no need for any PIA). If a PIA is required, the project managers will follow the organisational standard risk processes while doing the PIA. These processes require the evaluation of privacy risks not only from a corporate point of view (e.g., loss of reputation) but also from the individual point of view (i.e., via consultation with external stakeholders, citizens). Furthermore, any newly identified privacy risks will be included in the organisation's corporate risk register for future reference and managed in accordance with the organisation's risk standard processes.

	"Open doors" for privacy impact assessment integration	**Explanation**
1	Project initiation: privacy risk assessment	The focus is to perform a privacy risk assessment at the start of each project. This will trigger a PIA if the organisation's information governance corporate group determines that the project involves privacy risks.
2	Corporate level: incorporation of privacy risks into corporate risk registers and categories of risks	Privacy risks are incorporated into the corporate risk register. In addition, the corporate risk register is updated if new privacy related risks are identified by project managers during the PIA process.

Experience with the ICO PIA guidelines

The respondent found the ICO PIA Handbook and guidelines to be useful. However, he also pointed to a few limitations. Although he used the ICO guidelines to design the initial screening questions, he felt that the questions were too many and too focused on the technical side of privacy. Since the organisation does not deal with major IT developments (e.g., IT platforms and/or databases), he reduced the number of questions needed for the screening and adapted several of them to meet the organisation's needs.

In addition, the respondent found that ICO Handbook does not make sufficiently clear why PIAs are beneficial, while putting forward a PIA process that appears to be very complex. The

[207] The information governance group includes all of the directors across the organisation who are in charge of a specific business function and report to the risk information owner.

Handbook readers are left with the impression that the PIA process always requires a full scale assessment. He stressed that: "Only if you start reading the guidelines do you realise that you do not need to follow everything and that there are things that you do not need to do as part of your PIA. However, you need to read the full Handbook in order to decide what you need to do."

	Identified barriers to the use of the ICO PIA Handbook	Respondent's recommendations for improving the ICO PIA Handbook
1	Too many initial pre-assessment questions	Fewer pre-assessment questions and simpler process
2	PIA guidelines are too complex and mainly focused on the technical side of privacy	Simplify and shorten the PIA Handbook while putting more emphasis on the benefits of PIA
3	Handbook too focused on full-scale PIA	Greater focus on small-scale PIAs that can be easily implemented

Key lessons learned

Given that the organisation has just started to implement the new process, integrating privacy risks into existing project and risk management procedures, the respondent identified only one lesson learned. He underlined that an extensive and inclusive internal consultation, involving different parts of the organisation, is critical when defining the integration process. This will guarantee the full "buy-in" of all the interested and/or affected parties when the process is implemented.

Key motivations for integration

For the respondent, the key motivation for undertaking PIAs and integrating them more formally into the organisation's standard processes has been a cultural change within the organisation. Initially, the organisational focus was on information security only. Privacy impact assessment was not high on the organisational governance agenda. Only in more recent years has the organisation realised that information security and privacy are not the same things. As result, more executive attention has been given to privacy. This has also resulted in privacy being integrated into the organisational governance framework and processes.

8.1.6 Case study 6: Local government authority

Organisation's description

The organisation is a London borough comprising some established affluent areas as well as some recently emerging deprived and poor neighbourhoods. As is true of all London boroughs, the council is responsible for running most local services in its areas, such as schools, social services, waste collection and roads.

The council has a basic information charter, aligned to the Data Protection Act 1998, which sets the council's standards on the protection and safeguarding of personal data. In the charter, the council has made a few promises to its residents on how personal information, collected by the council, will be used and handled by council employees. Overall, the council has the

reputation of being a high-performing, high-achieving council in the UK. However, a few complaints were made by some residents under the Freedom of Information Act against this local authority, which the ICO investigated. These types of complaints appear to be a common occurrence within local authorities.

Experience with the integration of privacy risk

As stated in the organisation's response to the questionnaire, the council uses the British Standard on Risk Management, BS31100:2009,[208] as its main risk management methodology, but has its own internal project management approach, "which is a tailored version of PRINCE2". The council has, so far, completed two PIAs: one in relation to a project collecting data on employees and residents' re-cycling and waste disposal habits, and the second in relation to the creation and development of a citizens' account.

As stressed in the council's response to the questionnaire, the council has integrated privacy impact assessment into its own project management process as part of the procedure of completing the project initiation documentation. This process includes, early in the project life-cycle, an initial assessment on whether a PIA needs to be performed, and if so what scope the PIA should have, which the project manager, assigned to the project, does in conjunction with the assessment of the need for an Equality Impact Assessment (EqIA).[209] This initial screening is aligned with the ICO guidelines. The ICO recommended screening questions are answered and privacy risks assessed via a half-day internal workshop where the project manager, the data protection officer, the information security manager and other relevant council employees (i.e., head of the call centre, front line employees, etc.) discuss the screening questions, formulate the answers and finalise potential risks. Screening and a mini PIA are therefore undertaken in conjunction. The responsibility, for both initiating and completing the assessment, and implementing any resulting actions, lies with the project manager in charge of the project.[210] During the workshop, as stated by the respondent, the council uses "a risk based approach, taken from its information risk framework, in order to understand the risks and the legal framework". The respondent also underlined that, following the council's understanding of the ICO guidance, the council believes a full-scale PIA is only suitable for very large, national programmes and does not apply to local government. He emphasised that if a full PIA had been required for the two above-mentioned projects, the council would have stopped their implementation.

	"Open doors" for privacy impact assessment integration	**Explanation**
1	Project initiation: Project initiation documentation	Early in the project-life cycle, project managers are responsible to assess, via a workshop, whether a PIA is required and the level of privacy risks involved in their allocated projects. This initial assessment is integrated into the project initiation documentation.

[208] The BSI has withdrawn this standard, which has been superseded by ISO 31000.
[209] See the website of the Department for Work and Pensions: http://www.dwp.gov.uk/publications/impact-assessments/equality-impact-assessments/
[210] This is probably driven by the fact that the council has a risk team and information team but not a privacy team.

Experience with the ICO PIA guidelines

The respondent found the ICO PIA guidelines and Handbook useful. However, he also pointed to a few limitations. Although he used the ICO guidelines for the initial screening questions, he found that he often needed to adapt the questions in order for them to be relevant to the council's context. Furthermore, ICO guidelines provide little indications on what privacy requirements local authorities need to consider. Although requirements should emerge during the risk analysis, more directions on how to do the risk assessment, within local authorities, would be highly beneficial, given that often local authorities lack mature skills and knowledge on privacy risks.

He also stressed that the ICO Handbook gives organisations the impression that either they do not need a PIA or, if they do, the PIA will be a full-scale PIA requiring a complex and demanding effort (e.g., a long time frame and several resources). Greater emphasis, in the Handbook, on a middle level PIA, which is similar, in terms of resources and efforts, to a middle level EqIA and does not require more than 30 pages to be completed, will be useful to support PIA implementation and use within local authorities. Indeed, the respondent recommended that "privacy assessment should use the equality impact assessment as a model of how impact processes have been integrated into the council existing procedures and working" without requiring major efforts and new resources.

	Identified barriers to the use of ICO PIA guidelines	**Respondent's recommendations for improving the ICO PIA guidelines**
1	Initial pre-assessment questions are often not relevant	More tailored pre-assessment questions for local authorities
2	Guidelines provide no directions on risk requirements	Provide tools/directions on how to do the risk assessment
3	Handbook mainly focused on a full scale PIA	Simplify the PIA Handbook while putting more emphasis on middle level PIAs that can be easily implemented
4	PIA guidelines are too complex and give the impressions that PIAs require a lot of efforts	Use the equality impact assessment process as a model of how impact processes have been integrated into the council existing procedures and working.

Key lessons learned

Based on his experience at the council, the respondent identified a few lessons learned.

First, there is still a need for local authorities to fully embed privacy risks and PIAs into the council's central governance framework. Differently from EqIAs and equality rights, the council does not enforce PIAs as a key necessary requirement and/or regard privacy risks as a strong governance commitment. Indeed, the respondent feels that within the council "you cannot avoid to do an equality assessment but you can avoid doing a PIA".

Second, local authorities need to establish central PIA repositories where all the PIAs conducted by the council are stored and can be accessed. As in the case of equality impact assessment, where councils have established these repositories, this will promote a culture of sharing and benchmarking (i.e., councils can compare how well or badly they do in relation to privacy risks and PIAs), which in turn will support learning and self-improvement.

Key motivations for integration

The respondent identified the key motivator for doing PIAs and integrating PIA processes into existing council's procedures – i.e., the council's senior executives have given a clear direction that PIAs should be performed.

8.1.7 Case study 7: NHS acute hospital trust

Organisation description

The organisation is a NHS hospital providing a range of acute services. There are more than 5,000 full-time equivalent staff in the hospital making this organisation one of the largest employers in the area. In relation to its services, the hospital has 1,200 beds, 28 theatres and advanced critical care facilities services. Specifically, the hospital's emergency department is one of the busiest in the UK treating more than 120,000 patients each year.

The Trust has a well-developed confidentiality code of conduct and data protection policy, detailing how the Trust meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements are primarily based upon the Data Protection Act 1998; however, the Trust also refers to other relevant legislation and appropriate guidance, such as the NHS code of practice on confidentiality (2003). The Trust's data protection officer is currently the information governance manager, who is the primary person responsible for implementation of the Trust's data protection policy.

In 2012, the hospital won quality awards for some of its clinical services. The Trust has occasionally experienced patients complaining about lack of privacy and breach of confidentiality, but normally these complaints have been caused by patients feeling unhappy about the clinical care that they have received and therefore complaining also about confidentiality as part of the clinical procedure. The Trust has been reported twice to the ICO for privacy breaches that the Trust believes have been caused by human error.

Experience with the integration of privacy impact assessment

As stated in the organisation's response to the questionnaire, the Trust "has its own risk management tools and assurance process, which is consistently implemented" across the organisation. This makes use of the NHS Information Governance Toolkit. In relation to project management methodology, the Trust follows PRINCE2. The Trust has implemented its own PIA process and has currently undertaken three assessments since the introduction of the new PIA procedure (since September 2011).

In relation to integration, the Trust has integrated privacy risks into both its existing risk and project management approaches. From a risk point of view, the integration started by developing an information governance framework where the Trust defined clear responsibilities and a reporting structure for privacy risks. The framework splits into two streams: (1) information risks and processes, (2) and clinical risks and processes. Privacy risks sit within information risks; thus, the information risk owner has responsibilities for both information and privacy risks. Furthermore, the information risk owner is supported by 25 senior managers who are responsible for both information and privacy risks within their

business function. As stressed by the respondent, the 25 senior managers do not undertake PIAs, but they have instead "the responsibility to make sure that privacy risk is taken into consideration within their business function". The Trust also records many privacy-related risks in its own risk register and these are routinely monitored and reported by the information risk owner to relevant committees.

In addition to the Trust's governance framework and risk register, privacy risks, and specifically PIA, have also been operationally integrated into the NHS governance toolkit. This has been made easier, in recent years, by the fact that the toolkit has become much more prescriptive in relation to privacy risks. The integration into the toolkit has been achieved via an easy pre-screening assessment, which is based on three criteria weighing whether a PIA is required. The three criteria are whether: (1) a new project and/or proposal introduces any new piece of IT that deals with personal data, (2) a new process is introduced that was previously done anonymously, and (3) a new project and/or proposal involves changes in the way the Trust handles a huge amount of data about one individual or small changes involving several individuals. This pre-assessment should be done by the project manager for all new projects and contracts and is triggered even before the project initiation, when the project manager is developing the business case for the project. If any of the three criteria applies, then the project manager has to complete a PIA and refer the project to the information governance steering group. The information governance steering group will sign off the PIA and agree the mitigating actions to be implemented by the project manager to reduce the risks.[211] During the completion of the PIA, the data protection officer will be involved in drafting the assessment together with the project manager responsible for the project, and advising on the information and privacy risks involved as well as possible mitigating actions. The respondent's intention is also to extend the PIA integration into the project management process further than the business case by tightly integrating, in the near future, the PIA process into "the overall ICT project management process and the Project Management Office's methodology".

	"Open doors" for privacy impact assessment integration	**Explanation**
1	Pre-project and procurement requisitions: Business case	When completing the business case for a project or/and contract, project managers are responsible to assess, via an easy three-criteria assessment, whether a PIA is required.
2	Risk analysis: Information governance toolkit and assessment	The three-criteria pre-assessment is integrated into the main risk approach used by the organisation, the NHS information governance toolkit.
3	Governance framework: Governance responsibilities and reporting structure	The Trust has formally integrated privacy risk responsibilities and reporting into its own governance framework.
4	Corporate level: incorporation of privacy risks into the corporate risk register	Privacy risks are part of the Trust's risk register.

Experience with the ICO PIA guidelines

[211] The Trust is still discussing some components of the new process. The information governance steering group feels that it should be the one with the last say on privacy risks and recommendations. In addition, the Trust has not made the new information governance toolkit prescriptive yet.

When the Trust looked at the ICO PIA Handbook, the feeling was, as stressed by the respondent, that "they were too heavy going". Therefore, the Trust developed its own PIA process and documentation by "extracting" from the Handbook a workable procedure, which could be both meaningful and applicable to the health sector. The emphasis was on developing an easy-to-implement PIA process, both for the screening and the full-scale assessment. As mentioned previously, the screening process is based on three criteria, while the PIA template comprises four main sections (an introductory section on the project, a section on technology, a section on data sharing and a final section on information and privacy risks). The PIA template does not require more than a couple of hours to be completed. Overall, the respondent stressed that "although the ICO code of practices are useful, the ICO guidelines are too complex, too many, and too much to digest and turn into workable practices. The PIA process needs to be quick and easy, otherwise it is not going to happen within organisations and the relevant people will not be engaged." The problem is that within organisations, project managers are under competing pressures to deliver and, as a result, they constantly prioritise their activities and objectives. In order for them to undertake PIAs, the PIA process needs to be easily integrated into their normal working practices.

	Identified barriers to the use of ICO PIA guidelines	**Respondent's recommendations for improving the ICO PIA guidelines**
1	Initial pre-assessment questions are too many	Fewer and more tailored pre-assessment questions for NHS trusts.
2	Handbook and guidelines are too complex and too many	Simplify the PIA Handbook while putting more emphasis on an easy and workable PIA process.

Key lessons learned

Based on his recent experience within the Trust, the respondent identified a few lessons learned. First, unless the organisation follows a single project management process, it is often problematic to effectively embed a PIA into the organisation's fragmented project management framework. Therefore, the implementation of a single project management approach within the organisation is critical.

Second, it is very important for an effective implementation of the PIA process to get the internal buy-in from all the project managers. The organisation needs to deliver a clear message to all project managers that the PIA process must be followed and that PIAs are an organisational requirement.

Third, PIA processes and tools need to be constantly adapted and monitored and this should be based on privacy outcomes. Even if sophisticated PIA tools and processes are in place, there are still things that the organisation cannot foresee and/or predict from the start.

Key motivations for integration

The respondent identified the key motivations for doing PIAs and integrating PIA processes is the need to protect both the organisation and its patients. Furthermore, PIA is a good business practice since effective business benefits are to be gained from planning and addressing potential problems from the start instead of solving them when it is too late and things have already gone wrong.

8.1.8 Case study 8: Central government, ministerial department

Organisation's description

The organisation is a ministerial department. This public body has a basic privacy policy and an information charter, which are both based on the Data Protection Act 1998. The policy and charter are applicable to anyone who has dealings with the Department, whether through correspondence, involvement in public policy consultations or for any other reason, and set out the standards that the Department follows when dealing with personal information. The policy and charter require that information, which the Department collects from citizens, can only be used for the purpose clearly described to them and will not be passed to any other government department or third party unless citizens have given specific permission to do so or this information could be used to develop better public services.

The department has a small data protection team that looks after privacy and data protection issues, which might affect the working of the Department.

Experience with the integration of privacy risk

In relation to project management approaches, the organisation uses an adaptation of PRINCE2 as its main project management methodology. For risk management, this public body bases its approach both on HMG Information Assurance Maturity Model and the wider HMG Security Policy Framework.

As stated in the organisation's response to the questionnaire, privacy risk is integrated into the Department's existing processes via the "information asset risk assessment", which is the responsibility of the information asset risk owner. This assessment includes questions on PIAs such as: were PIAs required and/or carried out for specific initiatives. The Department does the assessment annually and, as stated by the respondent, the assessment should also drive further actions on how to better integrate privacy risks and PIA processes into the organisation. From an operational and project management point of view, a PIA process has not been formalised. This means that information service staffs, policy leads and/or project managers might decide autonomously that a PIA needs to be undertaken for their assigned initiatives and they can contact the data protection team. An internal PIA will then be done usually through an internal workshop where the data protection team and other relevant internal stakeholders will assess risks and mitigating actions.

The Department's intention is to develop a more formalised process and allocate clear responsibilities for privacy risk and PIA in the near future.

	"Open doors" for privacy risk integration	Explanation
1	Corporate level: Annual information asset risk assessment	Privacy risk is incorporated into the annual information asset risk assessment where the organisation assesses whether privacy risks have been properly managed and PIAs undertaken when required.
2	Project cycle: ad-hoc requests	The organisation has not implemented a proper, formal process or integration.

	"Open doors" for privacy risk integration	Explanation
		Information service staffs, policy leads and/or project managers are left on their own to decide whether their initiatives might involve privacy risks.

Experience with the ICO PIA guidelines

The respondent pointed to a few limitations in relation to the ICO PIA guidelines and Handbook. She found that the ICO guidelines had been difficult to implement within the Department, while the Handbook was "too dense" and complex. The respondent underlined the need for simplicity and "going back to a basic approach" that can be both workable and easy to implement. In addition, the respondent believes that in new and innovative data developments (i.e., big data), privacy and PIA should be presented and structured as a business enabler rather than a barrier. Therefore, the ICO guidelines should put more emphasis on PIA as an enabler and adding value process.

	Identified barriers to the use of ICO PIA guidelines	Recommendations for improving the ICO PIA guidelines
1	PIA guidelines are too complex and dense	Simplify and shorten the PIA Handbook while putting more emphasis on a basic PIA approach
2	Handbook is not enough focused on business benefits	Design PIA as a business enabler

Key lessons learned

Given that the organisation has not started a formal integration yet, the respondent identified only a few lessons learned. She underlined that the cultural component, involving privacy and internal organisational culture, is important and needs to be addressed not only through privacy or PIA training. In addition, ensuring the "buy-in" of the most senior people within the organisation is a necessary pre-condition for a successful integration of privacy risks and PIA into the organisation's existing processes.

Key motivations for integration

For the respondent the key motivations for undertaking PIAs and integrating more formally privacy risks into the organisation's standard processes have been the organisation's awareness of the importance of managing privacy risks as well as the changes in the regulatory and compliance environment.

8.2 CASE STUDIES: EXPERIENCE WITH POLICY-MAKING AND APPLICATION OF PIA

The ICO has an interest in encouraging the use of PIA in the formulation of policy. If privacy considerations are taken on-board early enough, there is less risk that the government will adopt policies that the public or other stakeholders will regard as intrusive. As unduly intrusive policies are likely to have electoral consequences, government should share the ICO's interest in evaluating proposed policies for their privacy risks and determining ways to address those risks before they become an electoral liability or before they exert downward pressures on the government's standing in public opinion polls.

While it might seem obvious that policy-makers would want to take privacy considerations into account, especially since compromises of privacy are daily fare in the media, in fact, the policy-making process is such that privacy gets less consideration than it should.

A study prepared for the ICO in 2009 provides some good insights into the policy-making process in the UK.[212] We cite some key observations from that report here. We then present four case studies on PIA and policy-making based on interviews with senior officials from central government departments. The findings from the case studies are congruent with the 2009 report. Beyond the congruence, however, our interest in both the 2009 report and our case studies is to see what insights we can glean on how the ICO might be able to gain more visibility for PIA in the policy-making process.

So with regard to the 2009 report, first we highlight some of its descriptions of the policy-making process and then see what we can derive from those descriptions as to where the ICO could insert itself or PIA into the process.

Where and how to insert PIA into the policy-making process is not an easy task in good part because there are no formal rules or guides to the policy-making process. As the 2009 report points out, "A significant amount of what goes on in Whitehall is driven by 'custom and practice', rather than formal rules. So in relation to policy, while there is a broad consensus on what policy is and 'how things should be done', there is no definitive guide."[213] While the manifestos of the political parties spell out their policy intentions, a good deal of policy is ad hoc and reactive, as the report confirms: "A considerable amount of Government policy is developed in response to 'events'. The recent banking crisis has been a good example of Government having to make its policy 'on the hoof'."[214]

In addition to the party manifestos and current events, policy-making is influenced by various factors. "Increasingly policy is multi-sourced, with much stronger roles for external bodies (treating the political parties as external in this context) of various sorts… Think-tanks have become steadily more influential in policy generation. So policy making no longer follows a single set model but is developed in different ways for different issues."[215] Ministers "take ideas from a variety of sources (stakeholders, lobbyists, think-tanks, the press, backbenchers)

[212] Walter, Peter, R.M. Morris and Duncan Simpson, *Understanding the Formulation and Development of Government Policy in the context of FOI*, Prepared for the Information Commissioner's Office by The Constitution Unit, University College London (UCL), 11 June 2009.
[213] Walter, Peter, R.M. Morris and Duncan Simpson, Understanding the Formulation and Development of Government Policy in the context of FOI, Prepared for the Information Commissioner's Office by The Constitution Unit, University College London (UCL), 11 June 2009, p. 7.
[214] Ibid., p. 11.
[215] Ibid., p. 16.

and ask for advice from the civil service machine on those ideas, authorising further and more detailed work where the idea seems promising."

Hence, while Ministers initiate and impel policy and the policy-making process, it is evident that other factors shape specific policies and influence the policy-making process. The 2009 report also makes clear that the process has evolved over the years too. A wider range of stakeholders are involved.

> It is almost impossible to imagine any project plan for a specific initiative, not discussing 'stakeholder engagement'… there is now a very clear expectation in Whitehall and Westminster that policy development should involve both formal and informal consultation with the public at large and those affected by the policy in particular.
> This is driven both by increasing expectations in society that the political process should be more open and by a growing view in government that policies which have not been exposed to public scrutiny at the outset are less likely to work effectively in practice. So 'discussion' documents are now much commonly utilised in policy making.[216]

The report goes on to identify and describe the role of some of the key different stakeholders who make policy. These include first and foremost government ministers, of course, special advisors to the ministers, departmental officials, the Treasury (which controls the governmental purse strings), the European Union, government agencies (and regulators, in particular). So to make sure privacy is taken into account in the policy-making process at the policy-formulation stage, the ICO would do well to "get at" ministers, to "bend their ear", i.e., to speak to them, to lobby them, to raise their awareness of the importance of taking privacy into account. However, there are lots of demands on ministers' time, so reaching ministers is a major challenge and, even if the ICO were successful in arranging a meeting (for example) between the Information Commissioner and the Minister, getting more than a few minutes of time would be difficult. However, reaching out to the special advisers (the SPADs) seems rather more fruitful. The report distinguishes two types of SPADs: the subject matter specialist and the political adviser. Special advisers often write the minister's speeches, which, as mentioned above, can be rather important policy-making instruments. "SPADs also have more time available than the Ministers themselves, so it can often be possible to discuss an issue in some depth with them before the submission is written, again saving time. SPADs can also usually articulate the direction of their Minister's thinking clearly."[217] Thus, the ICO could usefully spend some resources in identifying, contacting and "educating" special advisers about privacy issues generally and PIAs in particular and the need to take PIAs into account when the Minister initiates a new policy.

Another good possibility that might help ensure that PIA is taken into account would be for the ICO to identify and contact those who devise the communications plans that accompany new policies. The 2009 report states that "A communications plan will need to be developed for any announcement; and the communications team engaged. (It is one of the mantras of modern policy making that communications must be thought of from the outset of any policy consideration.)"[218] Thus, if the ICO could interact with those officials who devise the communications plans and convince them that privacy considerations and PIAs should be an element in the communications plan, then the time spent influencing the communications specialist might also be a good investment.

[216] Ibid., p. 29.
[217] Ibid., p. 38.
[218] Ibid., p. 40.

While we would recommend the ICO take these measures any way, their utility could be somewhat moot if Article 33 of the proposed Data Protection Regulation comes into force. The 2009 report points out that "an increasing amount of Whitehall policy making now has a marked European dimension, with the power of decisions, to a greater or less degree, having been elevated to the institutions of the European Union".[219] Article 33 will make "DPIAs" mandatory. Hence, in theory, PIAs (or DPIAs) will be required for any projects, whether from the government or private sector. However, nothing should be taken for granted. There are some issues yet to be clarified. Will "projects" include policies and legislative and regulatory initiatives? Will policy-makers know enough to take PIAs into account when formulating policy? Who will exercise that oversight or "watchfulness" to make sure PIAs are taken into account?

Perhaps the best way of ensuring that PIAs are undertaken when new policies are being devised is to make them a compulsory accompaniment of budgetary submissions for new policies, programmes and projects, as is the case in Canada. In other words, before anything is funded, the Treasury department has to see a PIA.

8.2.1 Case study 9: PIA and policy-making

Organisation's description

The organisation is a ministerial department. This public body has a basic privacy policy and an information charter, which are both based on the Data Protection Act 1998. The policy and charter are applicable to anyone who has dealings with the Department, whether through correspondence, involvement in public policy consultations or any other reason, and set out the standards that the Department follows when dealing with personal information. The policy and charter require that information, which the Department collects from citizens, can only be used for the purpose clearly described to them and will not be passed to any other government department or third party unless citizens had given specific permission to do so or this information could be used to develop better public services.

The department has a small data protection team that looks after privacy and data protection issues.

Experience with privacy risks and PIA applying to policy-making

The respondent regards the use and integration of PIA into the decision-making process as an important component for managing and addressing privacy risks early on in the implementation cycle. By performing privacy risk assessment during the ideation phase, there is a wider scope to avoid future privacy risks and therefore address privacy in a cost-effective way. However, even if the benefits for privacy are several, the respondent underlined that at present very little is done in relation to the assessment of privacy risks and application of PIA to the development of new policies. Based on her experience, occasionally a policy lead or minister might contact the data protection team to ask for advice and recommendation on possible privacy implications of a new policy and/or regulation. However, this involvement is on an ad hoc and random basis. There is not a systematic process in place and as a result

[219] Ibid., p. 41.

privacy risks could be assessed much later in the process or not at all, even for policies that could impact privacy. Furthermore, there is no systematic approach on how to do a PIA in the context of a new policy. The few privacy assessments undertaken for new policies can vary significantly. The involvement of the data protection team also appears to be more likely to happen when a policy implies the development of a new IT asset, such as a database or system.

As stated by the respondent, the reasons for poor consideration of privacy risks within and application of PIA to the policy-making process vary from the "complexity of the policy making picture", involving several ministers and bargaining consultations, to the need "to get on" with policy-making and delivery of the final outcome. An embedded culture where ministers feel that they have all the answers and where privacy is not on the top of the agenda also play a part in hindering and delaying the integration of privacy risks into the policy decision-making process. Indeed, the respondent indicated that differently from cyber-security, which is now a main focus of several government departments and ministers, privacy has never been a priority on the ministerial agenda.

	Present application of PIA to policy-making process	**Barriers to PIA application**
1	Ad hoc and random	Complexity of the policy picture
2	Not internal process in place	Pressure on delivering the end policy
3	Not systematic	Ministerial culture and ministers' mind set
4	Occasionally happening	Privacy is not regarded as a priority on the policy agenda

What next?

The respondent pointed to a few possible actions that could be taken, either by government departments and/or the ICO, to promote the use of PIA in the context of new policies and regulations. First, cultural barriers within departments need to be addressed. This calls for clearer and stronger directions and guidelines from the ICO to the ministers underlining the importance of such assessment while developing new policy and regulations. Second, from an operational point of view, PIA should be integrated within the existing regulatory impact assessment (RIA), which is an assessment tool, already in use within government departments, helping decision-makers understand the potential positive and negative effect of contemplated interventions. RIA has features in common with PIA, and offers a process, already in use within departments, which can be easily extended to include privacy risks.

	Possible next steps for improving the application of PIA to decision-making
1	Clearer ICO guidelines and directions in relation to privacy and policy-making
2	A PIA that can be easily integrated into the existing regulatory impact assessment

8.2.2 Case study 10: PIA and policy-making

Organisation's description

The organisation is a ministerial department. The Departments has an internal, general privacy policy, based on the Data Protection Act 1998, and several codes of practices related to how the Department and its employees should handle personal information and publication of public data. The Department has also recently endorsed an open data strategy aiming at creating a new era of accountability and openness in government by publishing accessible and reusable open data. The objective of the strategy is to drive reform and service improvement through transparency and greater participation from citizens, communities, partner groups and small businesses.

The Department has a data protection team that supports the whole Department and its different policy units.

Experience with privacy risks and PIA applying to policy-making

The respondent regards the use and integration of PIA into the policy-making process as a good practice, which can reduce the risk of policy-makers going in the "wrong directions" and can therefore address potential privacy risks early in the policy process. At present, in the Department, the application of PIA to new policies and/or regulation is not formalised and tends to occur on an ad hoc basis. Based on the respondent's experience, the process is often triggered by "someone", normally quite senior, within the policy team, who recognises the need for further investigation on the possible privacy implications of a new regulation and/or policy. As a result, he or she will involve the data protection team who will perform an assessment of the privacy risks, often in the form of "a discussion on privacy". On average, the data protection team will be involved in providing advice to policy teams on new policies and regulations three times a year. The respondent recognised that this is not perfect approach, leaving space for potential gaps in the way in which privacy risk is applied to policy-making, even when a regulation and/or policy might have clear implications on privacy. However, for the respondent, gaps are often the result of a lack of privacy awareness and/or understanding of how regulations and policies could impact privacy by a few policy-makers rather than an unwillingness to take privacy into consideration.

	Present application of PIA to policy-making process	Barriers to PIA application
1	Ad hoc and not systematic	Lack of awareness of privacy risks by a few policy-makers
2	No internal process in place	Lack of understanding of how policies and regulation could impact privacy by a few policy-makers

What next?

The respondent believed that, in order to promote the use of PIA in the context of new policies and regulations, a formalised process, requiring assessments at specific points in time during the policy-making development, is not going to be the solution. This will translate into creating unnecessary paper trails for policy-makers, who are already under different and diverse policy and bargaining pressures and, as result, do not want to deal with additional

processes or internal documentation. Instead, the respondent suggested that the emphasis should be on increasing awareness and understanding of privacy risks with policy-makers and providing them with training on privacy and new regulations in order for them to effectively recognise when they needed to involve the data protection team. Furthermore, although the respondent felt that she could not properly comment on whether PIA could and/or should be integrated into existing regulatory impact assessment (RIA) processes, her initial thoughts indicated that PIA for policy-making might be better approached as an autonomous and independent assessment instead of being part of an integrated regulatory impact process.

In relation to possible ICO interventions to promote the use of PIA in the context of policy and regulation, the respondent indicated that the ICO's PIA guidelines are too complex, "are too much to read" and provide too many rules when dealing with policy-makers who are focused on delivering new policies. As a result, the guidelines have not been used "a great deal" in the Department. However, the respondent also pointed out that an easy and simplified version of guidelines, specifically designed for policy-making and compressed in one page, could be quite useful. This is in line with the need for developing more specific PIA guidelines, which are more in tune with different types of users' requirements and needs. Possibly, this should be done by the ICO since, as indicated by the respondent, "if the ICO is not doing it, it is not going to happen".

	Possible next steps for improving the application of PIA to decision-making
1	One page, simple and easy PIA guidelines designed for policy-making
2	Increase awareness and understanding of privacy risks with policy-makers
3	Provide training on privacy and new regulation to policy-makers

8.2.3 Case study 11: PIA and policy-making

Organisation's description

The organisation is one of the smallest ministerial departments within the UK government. The Department's responsibilities encompass several key areas of government, with its decisions potentially exerting some influence on the working of several other public departments and agencies. The Department tends to focus on high-level policies and/or regulations, and deals with few policy areas that directly involve the handling and/or use, at any level, of personal data. It also holds little personal data in respect of citizens, with the exception of two sensitive areas where it keeps personal data, and has a very limited interface with the public. However, although its policies and regulation are at high and macro level, when operationalised by other departments they could influence individuals and therefore might have an impact on their privacy.

The Department applies the Data Protection Act 1998 when dealing with personal data, follows a specific risk management approach, which has been specifically developed for governments departments, and does not have a dedicated data protection team. However, both the security team and several information security policies have a privacy focus.

Experience with privacy risks and PIA applying to policy-making

Based on the respondent's experience, at present, in the Department, the application of PIA to new policies and/or regulations is not formalised and/or standardised. It tends to occur occasionally and on an ad hoc basis, when the policy team recognises that there might be a

relationship between a new regulatory development and privacy. The respondent was not aware of the number of PIAs applied to policy-making that the Department has undertaken. The Department does not have an internal repository for PIAs and the respondent was not directly involved in any.

The respondent emphasised that the privacy aspects of policies and regulations should never be ignored. However, he felt that more operational government departments, rather than strategic departments, should be responsible for and "taking care" of the PIA component of new policies and regulations. He also recognised that doing privacy assessment for policies and regulations is not an easy task, above all in departments, such as his, where the focus is on the macro (i.e., the country) rather than the micro level (i.e., citizens). He pointed out that PIAs, by their nature, require more and specific inputs from the micro, operational level, rather than the macro, high level. Furthermore, the respondent underlined that decision-makers tend not to be expert on privacy since their core activity centres around the development of macro and high-level policies directed to the good of the country rather than individuals.

In addition to the barriers to the application of PIA to policy-making already mentioned (e.g., the different nature and focus of PIA and policy-making, decision-makers' lack of experience in privacy), the respondent pointed out a few other important factors hindering the use of PIA for policy-making in the Department. Lack of departmental resources and the new government's emphasis on core business, all driven by recent public cuts and austerity, remain important barriers, together with the lack of an internal policy that clearly indicates the need for considering privacy risk and PIAs when developing new policies.

	Present application of PIA to policy-making process	**Barriers to PIA application**
1	Ad hoc and random	Policy-makers' lack of experience regarding privacy and PIAs
2	No internal process in place	Different nature of PIA and policy-making (i.e., the former focuses on the micro while the latter on the macro level)
3	Not systematic	Lack of resources and existing departmental focus on core business
4	Not standardised	Lack of internal policy and guidelines on privacy risks and assessment for policy-making

What next?

The respondent believed that, in order to promote the use of PIA in the context of new policies and regulations, departmental internal policies should clearly state that there is a need to take privacy risks in consideration during the regulatory process, while providing tools and guidelines on how to do it. He emphasised that the Orange Book and possibly the Green Book are "the right place" for including policy-making-focused guidelines on privacy risks. This is because these two books are specifically directed to governments departments, which should comply with their guiding principles, while dealing with a wide range of government specific activities, including policy-making, and their relevant risks. Indeed, there is already the recognition that the Orange Book should include some sections on privacy risks and PIAs and

the expectation is that the Treasury will address this soon in the near future. Furthermore, the respondent also indicated that the ICO and the Department should work together on readdressing privacy and policy-making issues with "workable and pragmatic" guidelines instead of developing separate and independent books and guides on privacy risks. Specifically, in relation to the ICO's PIA Handbook, the respondent felt that for policy-making they need a different approach to the one put forward in the Handbook. The Handbook's emphasis, and traditionally PIA's emphasis, has been towards handling data and personal information, which is not conducive for policy-making. A specific policy lens should be used in order to develop policy-making-based privacy guidelines, which pay greater attention to the macro level.

	Possible next steps for improving the application of PIA to decision-making
1	Clear internal departmental guidelines addressing privacy risks in the context of policy-making
2	Workable and pragmatic PIA guidelines designed for policy-making applicable across departments
3	The ICO and the Treasury should work together to develop PIA guidelines designed for policy-making
4	The Orange Book and possibly the Green Book should address PIA and provide an ideal platform for PIA guidelines designed for policy-making

8.2.4 Case study 12: PIA and policy-making

Organisation's description

The organisation is one of the biggest ministerial departments within the UK government, dealing with and handling a huge amount of citizens' personal data. The Department plays a big role in public service delivery and serves more than 20 million citizen-consumers. It holds a great deal of personal data in respect of citizens and widely interfaces with the public. In relation to personal data, the Department may check information about citizens with other data it has and may obtain and exchange information about citizens from and with other organisations in order to check the accuracy of information, prevent or detect crime, protect public funds and use in research or statistics.

The Department's has a high-level privacy policy, based on the Data Protection Act 1998, and an information charter, which both set the Department's standards on the protection and safeguarding of personal data. The Department might also develop more specific policies as new privacy and data protection needs emerge, such as in the case of the audio and video recording policy, which will expand and further define its existing departmental standards. The standards set up in the departmental policies must be followed by each employee and contractor when handling personal information. The department has a data protection team that that looks after privacy and data protection issues, which might affect the working of the Department.

Experience with privacy risks and PIA applying to policy-making

Based on the respondent's experience, there is a need for consistently assessing privacy risks when developing policies and regulations. As some specific cases within the Department that the respondent clearly pointed out, even if new regulatory developments do not directly involve data and/or privacy, their operationalisation could have an impact on these areas. Therefore, addressing privacy risks and potential issues early in the policy-making cycle would be both useful and beneficial to avoid problems later on when it might be more difficult or too late to effectively solve them. Indeed, the respondent was inclined to a system where any new piece of policy and/or regulation should be required to undergo some type of privacy risk assessment.

In relation to the application of PIA to policy-making in the Department, the respondent emphasised that the Department is a large organisation with multiple and fragmented policy units. This means that although the Department has developed guidelines and documentation on PIAs and has experience of doing PIA applying to policy-making, there is still a lot of variation in the way in which PIAs are used and undertaken within the organisation. He underlined that "some policy units are engaged, are aware of the issues, know the departmental policies" and where to find the PIA guidelines and documentation. Consequently they will involve the data protection team, think about privacy risks and the potential need for a PIA when developing new policies and regulations. However, other units are not engaged, are not aware of the issues and do not know about internal policies and PIA documentation. Therefore, they will not take into consideration privacy risks and the potential need for a privacy assessment while working on new regulatory developments. As a result, within the Department, there is not a standardised process and/or approach on how to integrate or undertake PIAs in a policy-making context. This is further exacerbated by the fact that departmental policies and documentation on PIA still leave several practical issues open

since the emphasis is on what it should achieve rather than how to do it. This is particularly critical for the application of PIA to policy-making since it is still uncertain how this should work and what a PIA for policy-making should look like.

In addition to the barriers to the application of PIA to policy-making already mentioned (e.g., fragmented and complex organisational structure, lack of knowledge, awareness and experience by policy-makers, lack of clarity on how to do a PIA for policy-making), the respondent indicated other important cultural and organisational factors hindering the use of PIA for policy-making within the Department. These factors vary from "too much general information and documentation" to find and digest for policy-makers, to lack of information-sharing on performed PIAs and a ministerial culture where "Ministers are more interested in getting their own way rather than ensuring that regulations are followed ".

	Present application of PIA to policy-making process	**Barriers to PIA application**
1	Not systematic	Policy-makers' lack of knowledge, awareness and experience on privacy and PIAs
2	Not standardised	Fragmented and complex organisational structure
3	No internal process in place	Lack of clarity on how to do a PIA for policy-making
4	No clear and practical guidelines available	Overload of general PIA information and documentation for policy-makers
5		Lack of information-sharing on performed PIAs
6		Ministers' culture of getting their own way

What next?

The respondent believed that, in order to promote the use of PIA in the context of new policies and regulations, first the Government should make more obvious their importance in the policy-making context. Second, more practical information and guidance on how to do a PIA for policy-making should be provided. This should take the form of a "practical and realistic" manual on what you need to think of when doing a PIA for policy-making. Indeed, the respondent emphasised that a new, specific approach and process need to be designed for doing a PIA in policy-making compared to a "one-size-fits-all" put forward in the ICO's PIA Handbook. Third, public organisations should publish their performed PIAs in order to share experience and best practices.

Specifically, in relation to possible steps that the ICO could take to promote the application of PIA to policy-making, the respondent pointed out the ICO should develop much clearer and practical guidelines on PIA, which do not focus "on the interpretation of privacy legislation", but rather on how to manage privacy risks and what is the reasonable risk exposure for different organisations. He also stressed that in order to enhance the use of PIAs in general, not only for policy-making, different risk management pathways for different types of organisations would be more useful and practical than the present "one-size- fit-all" approach. This imply that ICO's PIA Handbook should be provide clear indications of what different

types of organisations should do rather than guidelines that can be open to different interpretations. A new format for the Handbook, based much more on a booklet style, would also significantly improve the Handbook by offering an easy way to select and find the right information for different readers. Furthermore, the respondent also believed that the ICO should be much more straightforward on what is expected from the different organisations, including consistently pursuing issues and problems when they occur and deal without fail with clear and consistent breaches of the regulation.

	Possible next steps for improving the application of PIA to decision-making
1	Government should make clear the importance of PIA for policy-making
2	A specific, practical and realistic approach and process for assessing privacy risks in the context of policy-making
3	Publish PIAs
4	Provide different risk management pathways for different types of organisations rather than "one-size-fit-all"
5	The ICO's PIA Handbook should be more like a booklet and provide clear and practical guidelines on what different organisations should do for managing privacy risks
6	The ICO should without fail pursue clear and consistent breaches of the regulation

ANNEX 4 – JANUARY 2013 QUESTIONNAIRE

Dear xxx

Trilateral Research is a London-based limited liability partnership, specialising in research and the provision of strategic, policy and regulatory advice on new technologies, privacy, trust, risk and security issues.

We are doing a study for the Information Commissioner's Office (ICO) on how privacy impact assessment (PIA) can be more closely integrated with an organisation's risk and project management practices. To inform this study, we are conducting a survey of UK organisations to find out about their current practice concerning risk management and PIA. In that regard, we would like to ask your data protection officer and/or risk manager the six questions listed below. Could you provide their e-mail address or forward this e-mail to them, preferably with a copy to me?

1. *Does your organisation follow a particular **risk management** methodology and/or standard (e.g., ISO 27000, ISO 31000, etc.)? If so, which risk management methodology and/or standard does your organisation use?*

2. *Does your organisation follow a particular **project management** methodology and/or standard (e.g., PMBOK, PRINCE2, etc.)? If so, which project management methodology and/or standard does your organisation use?*

3. *Does your organisation currently take account of privacy risks in the context of its overall risk and/or project management process?*

4. *Does your organisation perform privacy impact assessment (PIA) and, if so, how many PIAs have you done so far?*

5. *If not, do you think it would be possible to include PIA as part of your organisation's overall risk and/or project management process?*

6. *If relevant to your organisation, is there any collaboration between the risk manager or project manager and the data protection officer regarding privacy risk management?*

We will anonymise all responses to this questionnaire and will not disseminate individual responses to any third parties, including the ICO. We will delete all responses once the study is completed in May 2013.

It would be very helpful if we could have your response by early February. We will be happy to share the aggregated results of the survey with you.

Kind regards.

Dr Monica Lagazio
Associate Partner
monica.lagazio@trilateralresearch.com
www.trilateralresearch.com

ANNEX 5 – ANONYMISED RESPONSES RE NUMBER OF PIAS PERFORMED

The following table lists anonymised responses to the Trilateral questionnaire with specific regard to the number of PIAs each organisation has performed. Of the 148 responses received as of 25 March 2013, 100 indicated they had done PIAs.

Category	Type	Organisation's attribution number	**4.b** If so, how many PIAs have you done so far? DK=Don't know
Unknown		Respondent 1	DK
Unknown		Respondent 2	2
Unknown		Respondent 3	12
Unknown		Respondent 4	7
Unknown		Respondent 5	DK
Unknown		Respondent 6	2
Unknown		Respondent 7	43
Unknown		Respondent 8	4
Unknown		Respondent 9	2
Unknown		Respondent 10	DK
Private Company	Large	Respondent 11	8
Private Company	Medium	Respondent 12	10
Private Company	FTS100	Respondent 13	400
Private Company	Large	Respondent 14	DK
Private Company	FTS100	Respondent 15	15
Private Company	FTSE100	Respondent 16	DK
Private Company	Large	Respondent 17	1
Public	Central Government	Respondent 18	1
Public	Central Government	Respondent 19	2
Public	Central Government	Respondent 20	10
Public	Central Government	Respondent 21	100
Public	Central Government	Respondent 22	4
Public	Central Government	Respondent 23	10
Public	Central Government	Respondent 24	DK
Public	Central Government	Respondent 25	0
Public	Central Government	Respondent 26	DK
Public	Central Government	Respondent 27	19
Public	Central Government	Respondent 28	0
Public	Central Government	Respondent 29	23
Public	Central Government	Respondent 30	1
Public	Central Government	Respondent 31	DK
Public	Central Government	Respondent 32	0
Public	Central Government	Respondent 33	64

Category	Type	Organisation's attribution number	**4.b** If so, how many PIAs have you done so far? DK=Don't know
Public	Central Government	Respondent 34	500
Public	Central Government	Respondent 35	20
Public	Central Government	Respondent 36	1
Public	Central Government	Respondent 37	DK
Public	Central Government	Respondent 38	3
Public	Central Government	Respondent 39	1
Public	Central Government	Respondent 40	20
Public	Central Government	Respondent 41	6
Public	Local Authority	Respondent 42	25
Public	Local Authority	Respondent 43	6
Public	Local Authority	Respondent 44	DK
Public	Local Authority	Respondent 45	2
Public	Local Authority	Respondent 46	DK
Public	Local Authority	Respondent 47	1
Public	Local Authority	Respondent 48	1
Public	Local Authority	Respondent 49	DK
Public	Local Authority	Respondent 50	5
Public	Local Authority	Respondent 51	1
Public	Local Authority	Respondent 52	2
Public	Local Authority	Respondent 53	DK
Public	Local Authority	Respondent 54	178
Public	Local Authority	Respondent 55	3
Public	Local Authority	Respondent 56	2
Public	Local Authority	Respondent 57	DK
Public	Local Authority	Respondent 58	3
Public	Local Authority	Respondent 59	DK
Public	Local Authority	Respondent 60	5
Public	Local Authority	Respondent 61	2
Public	Local Authority	Respondent 62	0
Public	Local Authority	Respondent 63	DK
Public	Local Authority	Respondent 64	1
Public	Local Authority	Respondent 65	4
Public	Local Authority	Respondent 66	0
Public	Local Authority	Respondent 67	4
Public	Local Authority	Respondent 68	2
Public	NHS	Respondent 69	3
Public	NHS	Respondent 70	9
Public	NHS	Respondent 71	25
Public	NHS	Respondent 72	9
Public	NHS	Respondent 73	13
Public	NHS	Respondent 74	DK
Public	NHS	Respondent 75	11
Public	NHS	Respondent 76	DK
Public	NHS	Respondent 77	186
Public	NHS	Respondent 78	DK

Category	Type	Organisation's attribution number	**4.b** If so, how many PIAs have you done so far? DK=Don't know
Public	NHS	Respondent 79	DK
Public	NHS	Respondent 80	10
Public	NHS	Respondent 81	DK
Public	NHS	Respondent 82	0
Public	NHS	Respondent 83	6
Public	NHS	Respondent 84	34
Public	NHS	Respondent 85	54
Public	NHS	Respondent 86	10
Public	NHS	Respondent 87	1
Public	NHS	Respondent 88	21
Public	NHS	Respondent 89	6
Public	NHS	Respondent 90	DK
Public	NHS	Respondent 91	6
Public	NHS	Respondent 92	DK
Public	NHS	Respondent 93	DK
Public	NHS	Respondent 94	9
Public	NHS	Respondent 95	DK
Public	NHS	Respondent 96	DK
Public	NHS	Respondent 97	10
Public	NHS	Respondent 98	1
Public	NHS	Respondent 99	DK
Public	NHS	Respondent 100	0

ANNEX 6 – A SHORT BIBLIOGRAPHY OF UK PIA REPORTS

The following are the publicly available PIA reports discovered by Trilateral following an Internet search of some hours.

No.	PIA report	year	pages	source
1	Department of Finance and Personnel, Privacy Impact Assessment (PIA): The VLA Publication of the Capital Value: Domestic Valuation List in Northern Ireland, August 2006.[220]	2006	22	government
2	80/20 Thinking Ltd, Privacy Impact Assessment [for Phorm Inc.], 2008	2008	22	industry
3	National Policing Improvement Agency (NPIA), IMPACT Programme: Police National Database Privacy Impact Assessment Report, April 2009. http://www.npia.police.uk/en/docs/Privacy_Impact_Assessment.pdf	2009	42	government
4	Driver and Vehicle Licensing Agency, Privacy Impact Assessment for Continuous Insurance Enforcement Project, April 2009. http://www.dft.gov.uk/dvla/publications.aspx	2009	20	government
5	Black, Fiona, PIA Project Manager, Scottish Health Information Service – Privacy Impact Assessment Report, 16 Sept 2009.	2009	49	NHS
6	Office for National Statistics, Report of a Privacy Impact Assessment in relation to the 2011 Census England and Wales, November 2009. http://amberhawk.typepad.com/files/census_pia-final-version.pdf	2009	62	government
7	UK Anti-Doping, Report of a Privacy Impact Assessment conducted by UK Anti-Doping in relation to Personal Information disclosed to it by the Serious Organised Crime Agency, Final, 15 January 2010. http://www.ukad.org.uk/resources/document/privacy-impact-assessment	2010	12	government
8	Northern Ireland Statistics and Research Agency, Report of a Privacy Impact Assessment Conducted by the Northern Ireland Statistics and Research Agency in relation to the 2011 Census Northern Ireland, May 2010. http://www.nisra.gov.uk/archive/census/2011/Privacy%20Impact%20Assessment.pdf	2010	65	government
9	UK Border Agency, Report of a Privacy Impact Assessment conducted by the UK Border Agency in relation to the High Value Data Sharing Protocol	2010	38	government

[220] The Valuation and Lands Agency (VLA) is an agency of the Department of Finance and Personnel (DFP) in Northern Ireland.

No.	PIA report	year	pages	source
	amongst the immigration authorities of the Five Country Conference, undated [30 June 2010[221]]. http://www.ukba.homeoffice.gov.uk/sitecontent/documents/aboutus/workingwithus/high-value-data-sharing-protocol/pia.pdf?view=Binary			
10	Suffolk Mental Health Partnership NHS Trust, Privacy Impact Assessment (PIA) Guidance, Nov 2010. http://www.smhp.nhs.uk/LinkClick.aspx?fileticket=PitwGWr9978%3D&tabid=160&mid=582	2010	38	NHS
11	Scottish Government, eCare Programme, eCare/GIRFEC inter-Agency Communication Tool (iACT) Privacy Impact Assessment, Version 1.0 Release, 17 Nov 2010. http://www.scotland.gov.uk/Topics/Government/PublicServiceReform/efficientgovernment/DataStandardsAndeCare/pia	2010	116	government
12	Home Office, PIA Report re decriminalised convictions for gay sexual offences, January 2011. http://www.homeoffice.gov.uk/publications/about-us/legislation/freedom-bill/pia-report?view=Binary	2011	4	government
13	[Scottish] Improvement Service, National Entitlement Card (NEC) Privacy Impact Assessment Report, Revised, Jan 2011. www.entitlementcard.org.uk/docs/PIAJan2011.pdf	2011	11	government
14	Information Commissioner's Office (ICO), Privacy Impact Assessment Report Making the register available in a machine readable and reusable format, 16 May 2011. http://www.ico.gov.uk/about_us/consultations/~/media/documents/library/Corporate/Research_and_reports/pia_report_publication_of_the_dp_register.ashx	2011	31	government
15	Ministry of Justice, Abolition of the Legal Services Commission (a Non-Department Public Body) and the establishment of a new Executive Agency within the Ministry of Justice Privacy Impact Assessment Report, June 2011. http://www.justice.gov.uk/downloads/legislation/bills-acts/legal-aid-sentencing/pia-abolition-lsc.pdf	2011	25	government
16	Ministry of Justice, Information Gateway – Legal Aid: Privacy Impact Assessment Report, June 2011. http://www.justice.gov.uk/downloads/legislation/bills-acts/legal-aid-sentencing/pia-information-gateway.pdf	2011	20	government
17	Engage Consulting Limited, Privacy Impact Assessment: Use of Smart Metering data by Network	2011	77	industry

[221] The Home Office FOI team in an e-mail dated 8 Feb 2013 informed Trilateral that the PIA report was posted on the website on 30 June 2010.

No.	PIA report	year	pages	source
	Operators, Energy Networks Association, October 2011. http://www.energynetworks.org/modx/assets/files/news/consultation-responses/Consultation%20responses%202011/ENA%20Privacy%20Impact%20Assessment%20Use%20of%20Privacy%20Impact%20Assessment%20Use%20of%20Smart%20Metering%20data%20by%20Network%20Operators_Oct%202011.pdf			
18	Land Registry, Privacy Impact Assessment Report - Making price paid data available through publication in a machine readable and reusable format, March 2012. http://www.landregistry.gov.uk/__data/assets/pdf_file/0012/3351/ppd_pia.pdf	2012	15	government
19	Lynch, Ellen, Scottish Government, and Kathy McGregor, ISD Scotland, Scottish Care Home Census (SCHC) Privacy Impact Assessment, Version X, March 2012. http://www.scotland.gov.uk/Resource/0040/00401045.pdf	2012	19	government
20	Hill, Geoff, Regional Collaboration: Source & Covert – Privacy Impact Assessment Report, Devon & Cornwall Constabulary, 10 April 2012. http://www.devon-cornwall.police.uk/YourRightInformation/FreedomInformation/Documents/RegionalSCPrivacyImpactAssR.pdf	2012	23	police
21	UK Cabinet Office, Individual Electoral Registration: Privacy Impact Assessment Report, May 2012. http://www.cabinetoffice.gov.uk/sites/default/files/resources/Privacy-Impact-Assessment-090512.pdf	2012	26	government
22	Home Office, Privacy Impact Assessment of the Draft Communications Data Bill, 14 June 2012. http://www.homeoffice.gov.uk/publications/counter-terrorism/comms-data-bill/communications-data-privacy-ia?view=Binary	2012	25	government
23	APS Group Scotland, Aquaculture and Fisheries (Scotland) Bill - Privacy Impact Assessment, Scottish Government, November 2012. http://www.scotland.gov.uk/Resource/0040/00408277.pdf	2012	14	government
24	Home Office, DBS [Disclosure and Barring Service] Go-Live Privacy Impact Assessment (PIA), 27 Nov 2012 . http://www.homeoffice.gov.uk/publications/agencies-public-bodies/dbs/about-dbs/dbs-privacy-impact?view=Binary	2012	17	government
25	Department of Energy and Climate Change (DECC),	2012	27	government

No.	PIA report	year	pages	source
	Smart Metering Implementation Programme Privacy Impact Assessment, December 2012. http://www.decc.gov.uk/assets/decc/11/consultation/smart-metering-imp-prog/7226-sm-privacy-ia.pdf			
26	National Policing Improvement Agency, Police National Database: Privacy Impact Assessment Update Report, undated. http://www.npia.police.uk/en/docs/PND_PIA_update_report.pdf	ND	14	police

ANNEX 7 – COPYRIGHT

Various documents referenced in this report are copyright protected. These include the following:

Methodology	Copyrighted?
ICO PIA Handbook	No
RFID PIA framework	No
Article 33 of the proposed Data Protection Regulation	No
PIAF methodology	No
PIA of the Draft Communications Data Bill	No
PIA on smart metering implementation	Yes
PIA on the use of Smart Metering data by Network Operators	Yes
PIA on the Police National Database	Yes
PIA on the Police source and covert consolidated data system	No
PIA on the Five Country Conference Protocol on sharing fingerprint data	No
PIA on the eCare Inter-Agency Communication Tool	Yes
Project Management Body of Knowledge (PMBOK©)	Yes
PRINCE2 (PRojects IN Controlled Environments)	Yes
Agile	No
HERMES	No
ISO 31000:2009 Risk management — Principles and guidelines	Yes
Combined Code and Turnbull Guidance	Yes
UK Treasury's The Orange Book: Management of Risk	Yes
ENISA's approach to risk management	Yes
ISO/IEC 27005:2011 Information security risk management	Yes
IT-Grundschutz	No
NIST SP 800-39 Managing Information Security Risk	No
ISACA and COBIT	Yes
CRAMM	No
EBIOS	No
OCTAVE	Yes
NIST SP 800-30 Guide for Conducting Risk Assessments	No
ISO/IEC 29100:2011 Information technology — Security techniques	Yes
NIST SP 800-122, Guide to Protecting the Confidentiality of PII	No
CNIL methodology for privacy risk management	No

The Trilateral team has contacted the copyright holders and sought their approval for the team to paraphrase or quote from the copyrighted documents for this report. We have had positive responses from all, except for Carnegie Mellon re OCTAVE. We have not yet had a response, either positive or negative, from Carnegie Mellon. However, we are actively attempting to get permission and expect to have it before delivery of the final version of this report at the end of May.

Most of those from whom we sought permission to paraphrase or quote from their documents said we were free to do so as long as we gave a proper citation.

Crown copyright documents are covered by the Open Government Licence (OGL), which is "a free licence developed to enable freer use of government information and public sector information without the need for formal agreements or any registration transaction. This licence takes the form of a simple set of terms and conditions for re-use and can be viewed at

http://www.nationalarchives.gov.uk/doc/open-government-licence/open-government-licence.htm".

Regarding its PIA on the smart metering programme, the Department of Energy and Climate Change informed us that "This publication (excluding logos) may be re-used free of charge in any format or medium provided that it is re-used accurately and not used in a misleading context. The material must be acknowledged as crown copyright and the title of the publication specified."

All NIST publications are in the public domain and can be used freely by anyone.

ENISA welcomes our use of the material, provided that the original source is clearly referenced.

The Energy Networks Association (ENA) said they were happy to give permission to the ICO to summarise, paraphrase and quote from their PIA report.

In the instance of our paraphrasing of the ISO documents, BSI informed us that "The standard copyright requirement is that the document shows originality, and isn't simply a re-working of the text of the original work. We think that this does show that originality, so there are no copyright implications."

Re the Turnbull Guidance, the FRC gave us permission as follows: "© Financial Reporting Council (FRC). Adapted and reproduced with the kind permission of the Financial Reporting Council. All rights reserved. For further information, please visit www.frc.org.uk or call +44 (0)20 7492 2300."

Project Management methodologies including PMBOK, PRINCE2, and Agile are the subject of various studies and papers in the public domain. Where we have drawn on these for our review, we have provided full citations.

Where the Agile Manifesto and Twelve Principles are cited, they are reprinted by permission which is granted on the agilemanifesto.org website, which follows the text with the statement "© 2001, this declaration may be freely copied in any form, but only in its entirety through this notice." This citation, including a complete list of the authors, is included in this report accordingly.

CNIL welcomes our use of its material, provided that the original source is clearly referenced.

ANSI welcomes our use of its material (EBIOS), provided that the original source is clearly referenced.

The IT-Grundschutz Team from the German BSI welcomes our use of its material, provided that the original source is clearly referenced.

Henri Tudor Research Public Center welcomes our use of its material (schema for HERMES), provided that the original source is clearly referenced. Unité de pilotage informatique de la Confédération confirms that HERMES is a free, open source methodology and agrees to our use of its material, provided that the original source is clearly referenced.

REFERENCES – PROJECT & RISK MANAGEMENT STANDARDS

The following is a list of the references which were reviewed for this report. There are more references here than those analysed in Chapters 2 and 3.

International Organization for Standardization (ISO)

- International Organization for Standardization, *Information technology — Security techniques — Information security risk management*, ISO/IEC 27005:2008(E), First edition, Geneva, 15 June 2008.
- International Organization for Standardization, *Information technology — Security techniques — Privacy framework*, International Standard, ISO/IEC 29100:2011(E), First edition, Geneva, 15 Dec 2011.
- International Organization for Standardization, *Risk management — Principles and guidelines*, International Standard, ISO 31000:2009(E), First edition, Geneva, 15 Nov 2009.
- International Organization for Standardization, ISO 21500:2012 *Guidance on project management*, 3 Sept 2012.

Organisation for Economic Co-operation and Development (OECD)

- Organisation for Economic Co-Operation and Development (OECD), *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, Recommendation of the OECD Council at its 1037th Session on 25 July 2002, Paris, 2002. http://www.oecd.org/sti/interneteconomy/2494779.pdf

European Union

- European Network and Information Security Agency (ENISA), [Emerging and Future Risks] *EFR Framework Handbook*, Draft, Heraklion, March 2009.
- European Network and Information Security Agency (ENISA), [Emerging and Future Risks] *EFR Framework Introductory Manual*, Heraklion, March 2010.
- European Network and Information Security Agency (ENISA), *ENISA Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*, Heraklion, July 2010. http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia
- *The Privacy Impact Assessment Framework for RFID Applications*, Brussels, January 2011. http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf
- Art. 29 Data Protection Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, Brussels, Adopted on 11 February 2011. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

France

- Commission Nationale de l'Informatique et des Libertés (CNIL), *Methodology for Privacy Risk Management*, Translation of June 2012 edition, Paris, 2012. http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

- Commission Nationale de l'Informatique et des Libertés (CNIL), *Measures for the privacy risk treatment*, Translation of June 2012 edition, Paris, 2012. http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Measures.pdf
- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), *EBIOS Expression of needs and Identification of security objectives*, Paris, 2010. http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html

Switzerland

- Swiss Federal Strategy Unit for Information Technology (FSUIT), *Hermes: Management and Execution of projects in Information and Communication Technologies (ICT) Foundations*, Switzerland, 2003. http://www.isb.admin.ch

United Kingdom (UK)

- BSI, *BS 31100:2011 Risk Management: Code of practice and guidance for the implementation of BS ISO 31000*, 2011.
- Cabinet Office, *Information Technology Infrastructure Library (ITIL)*, Version 3, London, July 2011.
- Office of Government Commerce (OGC), *Managing Successful Projects with PRINCE2*, 2009.
- Her Majesty Treasury, *The Orange Book: Management of Risk - Principles and Concepts*, London, October 2004. http://www.hm-treasury.gov.uk/d/orange_book.pdf
- Information Commissioner's Office, *Privacy Impact Assessment Handbook*, Version 2.0, Wilmslow, 2009. http://www.ico.gov.uk/pia_handbook_html_v2/html/0-advice.html
- Financial Reporting Council, Internal Control, Revised Guidance for Directors on the Combined Code, October 2005. https://www.frc.org.uk/getattachment/5e4d12e4-a94f-4186-9d6f-19e17aeb5351/Turnbull-guidance-October-2005.aspx. See also: https://www.frc.org.uk/Our-Work/Codes-Standards/Corporate-governance.aspx
- Institute of Risk Management (IRM), *Risk Management Standard*, London, [n.d.]. http://www.theirm.org/publications/documents/ARMS_2002_IRM.pdf
- Institute of Risk Management (IRM), Association of Insurance and Risk (AIRMIC), and the Public Sector Risk Management Association (Alarm), A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000, London, [n.d.].

United States of America (USA)

- National Institute of Standards and Technology (NIST), U.S. Department of Commerce, *Guide for conducting risk assessment*, NIST Special Publication (SP) 800-30, Revision 1, Joint Task Force Transformation Initiative, Gaithersburg, MD, September 2012. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

- National Institute of Standards and Technology, U.S. Department of Commerce, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication (SP) 800-37, Joint Task Force Transformation Initiative, Gaithersburg, MD, February 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
- National Institute of Standards and Technology, U.S. Department of Commerce, *Managing Information Security Risk:Organization, Mission and Information System View*, NIST Special Publication (SP) 800-39, Joint Task Force Transformation Initiative, Gaithersburg, MD, March 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
- National Institute of Standards and Technology, U.S. Department of Commerce, *Building an Information Technology Security Awareness and Training Program*, NIST Special Publication (SP) 800-50, Joint Task Force Transformation Initiative, Gaithersburg, MD, October 2003. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
- National Institute of Standards and Technology, U.S. Department of Commerce, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53, Revision 4, Joint Task Force Transformation Initiative, Gaithersburg, MD, February 2012. http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf
- National Institute of Standards and Technology, U.S. Department of Commerce, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, NIST Special Publication (SP) 800-66, Revision 1, Joint Task Force Transformation Initiative, Gaithersburg, MD, October 2008. http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
- National Institute of Standards and Technology, U.S. Department of Commerce, NIST Special Publication (SP) 800-100, *Information Security Handbook: A Guide for Managers*, Joint Task Force Transformation Initiative, Gaithersburg, MD, October 2006. http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf
- National Institute of Standards and Technology, U.S. Department of Commerce, NIST Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (PII), Joint Task Force Transformation Initiative, Gaithersburg, MD, April 2010. http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
- ISACA, *Control Objectives for Information and Related Technology (COBIT) 5: A Business Framework for the Governance and Management of Enterprise IT*, 2012.
- Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) - Fourth Edition*, 2008.
- CMMI Product Team, *CMMI for Development, Version 1.3* (CMU/SEI-2010-TR-033). Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm

Other papers

- Saeed Abu-Nimeh, and Nancy R. Mead, *Combining Privacy and Security Risk Assessment in Security Quality Requirements Engineering*, AAAI Spring Symposium: Intelligent Information Privacy Management, 2010. http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/download/1037/1468

- Heckle, R.R., and S.H. Holden, *Analytical tools for privacy risks: Assessing efficacy on vote verification technologies*. In Symposium On Usable Privacy and Security. Poster. http://cups.cs.cmu.edu/soups/2006/posters/heckle-poster_abstract.pdf
- Cavoukian, Ann, Ontario Information & Privacy Commissioner, "Privacy by Design", 2009.
- Cavoukian, Ann, Ontario Information & Privacy Commissioner, "A Policy is Not Enough: It Must be Reflected in Concrete Practices", September 2012. http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1210

REFERENCES – FURTHER READING

Following is a short list of some of the Trilateral team's PIA-related publications.

Books

Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, The MIT Press, Cambridge, MA, 2006.

Wright, David, and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

Chapters in books

Bellamy, Christine, Charles Raab and Perri 6, 'Multi-agency Working in British Social Policy: Risk, Information Sharing and Privacy', in Miriam Lips, John Taylor and Frank Bannister (eds.), *Public Administration in the Information Society: Essays on Risk and Trust*, IOS Press, Amsterdam, 2006.

Finn, Rachel, David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert et al., *European data protection: coming of age?*, Springer, Dordrecht, 2013.

Raab, Charles and David Wright, "Surveillance: Extending the limits of privacy impact assessment", Chapter 17, in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

Wright, David and Paul De Hert, "Introduction to Privacy Impact Assessment", Chapter 1, in David Wright and Paul De Hert, *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

Wright, David and Paul De Hert, "Findings and Recommendations", Chapter 22, in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

Articles in peer-reviewed journals

6, Perri, Christine Bellamy and Charles Raab, "Information Sharing Dilemmas in Public Services: Using Frameworks from Risk Management", *Policy & Politics*, Vol. 38**,** No. 3, 2010, pp. 465-481.

Raab, Charles D., "Perspective: What DPAs Need to Know", *The Privacy Advisor*, IAPP, Vol. 12, No. 1, January-February 2012, pp. 27-28.

Raab, Charles D., and Colin J. Bennett, "The Distribution of Privacy Risks: Who Needs Protection?", *The Information Society*, Vol. 14, No. 4, October-December 1998, pp. 263-274.

Rodrigues, Rowena, David Wright and Kush Wadhwa and, "Developing a privacy seal scheme (that works)" *International Data Privacy Law*, Vol. 3, Issue 2, 2013.

Wadhwa, Kush, "*Privacy Impact Assessment Reports: A Report Card*", *Info*, Vol. 14, No. 3, pp. 35-47, May 2012.
http://www.emeraldinsight.com/journals.htm?issn=1463-6697&volume=14&issue=3

Wadhwa, Kush, and Rowena Rodrigues, "Evaluating Privacy Impact Assessments", *Innovation*, 2013.

Wright, David, "Should privacy impact assessment be mandatory?", *Communications of the ACM*, Vol. 54, No. 8, August 2011, pp. 121-131. http://cacm.acm.org/magazines/2011/8

Wright, David, "The state of the art in privacy impact assessment", *Computer Law & Security Review*, Vol. 28, No. 1, Feb. 2012, pp. 54-61.
http://www.sciencedirect.com/science/journal/02673649

Wright, David, and Charles D. Raab, "Constructing a surveillance impact assessment", *Computer Law & Security Review*, Vol. 28, No. 6, Dec 2012, pp. 613-626.

Wright, David, and Kush Wadhwa, "Introducing a privacy impact assessment policy in the EU Member States", *International Data Privacy Law*, Vol. 3 Issue, 1 February 2013.
http://idpl.oxfordjournals.org/content/early/recent.

Wright, David, Rachel Finn and Rowena Rodrigues, "A comparative analysis of PIA in six countries", *The Journal of Contemporary European Research*, Vol. 9, No. 1, March 2013..

Wright, David, Raphaël Gellert, Serge Gutwirth and Michael Friedewald, "Minimizing technology risks with PIAs, precaution and participation", *IEEE Technology & Society*, Vol. 30, Issue 4, Winter 2011, pp. 47-54.

Reports

Ball, Kirstie, David Lyon, David Murakami Wood, Clive Norris and Charles Raab, *A Report on the Surveillance Society*, Office of the Information Commissioner, Wilmslow, 2006

Raab, Charles, and Benjamin Goold, *Protecting Information Privacy*, Research Report 69, Equality and Human Rights Commission, London, 2011.

Raab, Charles, Kirstie Ball, Steve Graham, David Lyon, David Murakami Wood and Clive Norris, *The Surveillance Society – An Update Report on Developments Since the 2006 Report on the Surveillance Society*, Office of the Information Commissioner, Wilmslow, 2010. Reproduced in House of Commons Home Affairs Committee, *Information Commissioner's Annual Report to the House of Commons pursuant to the Home Affairs Committee's report 'A Surveillance Society', Fifth Report of Session 2007-08*, Fourth Report of Session 2010-11, HC 702, The Stationery Office, London, 1 March 2011.
http://www.publications.parliament.uk/pa/cm201011/cmselect/cmhaff/702/702.pdf

Raab, Charles, Perri 6, Anne Birch and Marina Copping, *Information Sharing for Children at Risk: Impacts on Privacy*, E-Care Programme, Scottish Executive Health Department, Edinburgh, 2004, 179 pp.

Wright, David, Kush Wadhwa, Paul De Hert and Darius Kloza, Privacy Impact Assessment Framework (PIAF), Deliverable D1 to the European Commission, Sept 2011. www.piafproject.eu

Website

PIAw@tch. http://www.piawatch.eu/