Legal Aid Agency

Data protection audit report

November 2021

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

The Legal Aid Agency (LAA) agreed to a consensual audit of its processing of personal data. An introductory telephone meeting was held on 9 August 2021 with representatives of the LAA to discuss the scope of the audit.

The LAA is an Executive Agency of the Ministry of Justice (MOJ). The LAA process personal data to exercise its own and associated public functions, which is to provide criminal and civil legal aid and advice in England and Wales as outlined by the Legal Aid, Sentencing and Punishment of Offenders Act 2012. The MOJ are the data controller for the personal data processed by the LAA and, therefore, ICO auditors reviewed documentary evidence and conducted interviews with staff from both the LAA and MOJ and have tested MOJ processing in so far as it relates to the LAA. The recommendations made in this report should therefore be viewed in that context.

The purpose of the audit is to provide the Information Commissioner and the LAA with an independent assurance of the extent to which the LAA, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of the LAA's processing of personal data. The scope may take into account any data protection issues or risks which are specific to the LAA, identified from ICO intelligence or LAA's own concerns, and/or any data protection issues or risks which affect their specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of the LAA, the nature and extent of the LAA's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to the LAA. It was agreed that the audit would focus on the following area(s)

Scope area	Description
Governance and Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
Information Security	There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore, the LAA agreed to continue with the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 19 October 2021 to 21

October 2021. The ICO would like to thank the LAA for its flexibility and commitment to the audit during difficult and challenging circumstances.

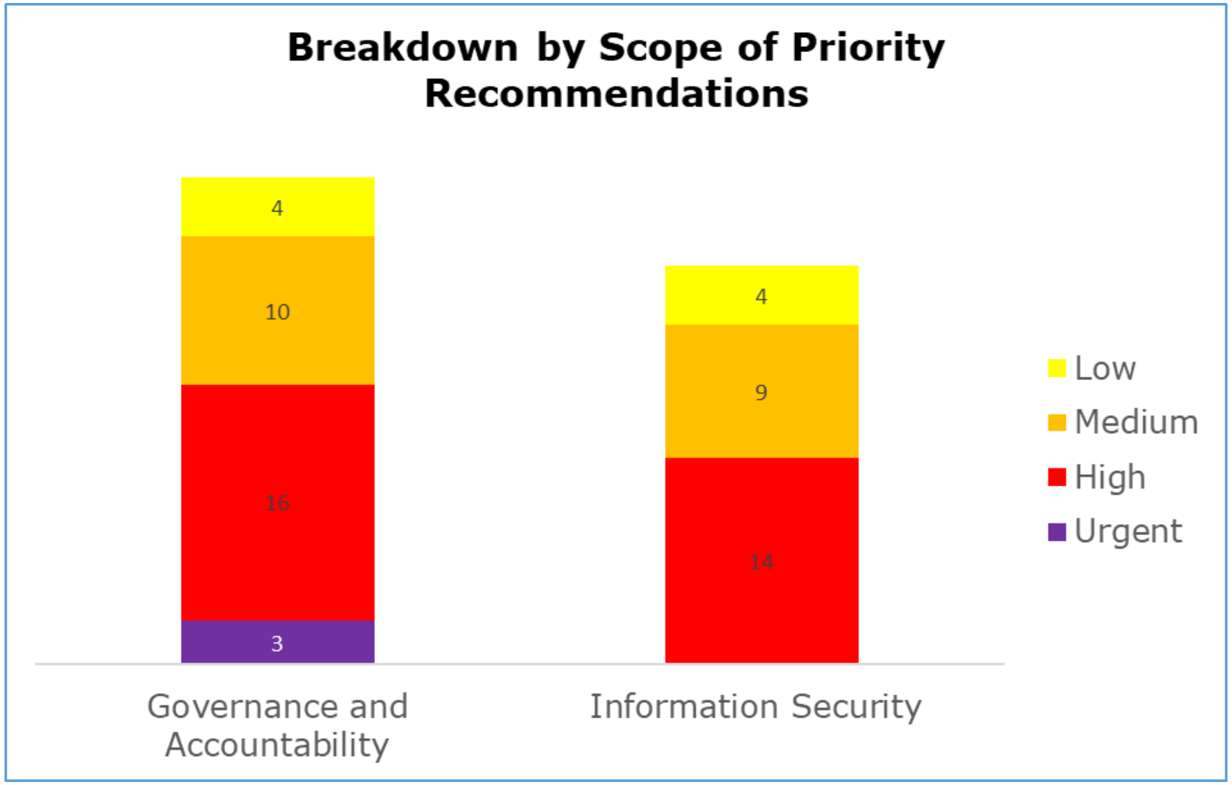
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the LAA in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. The LAA's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Governance and Accountability	REASONABLE	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Information Security	REASONABLE	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

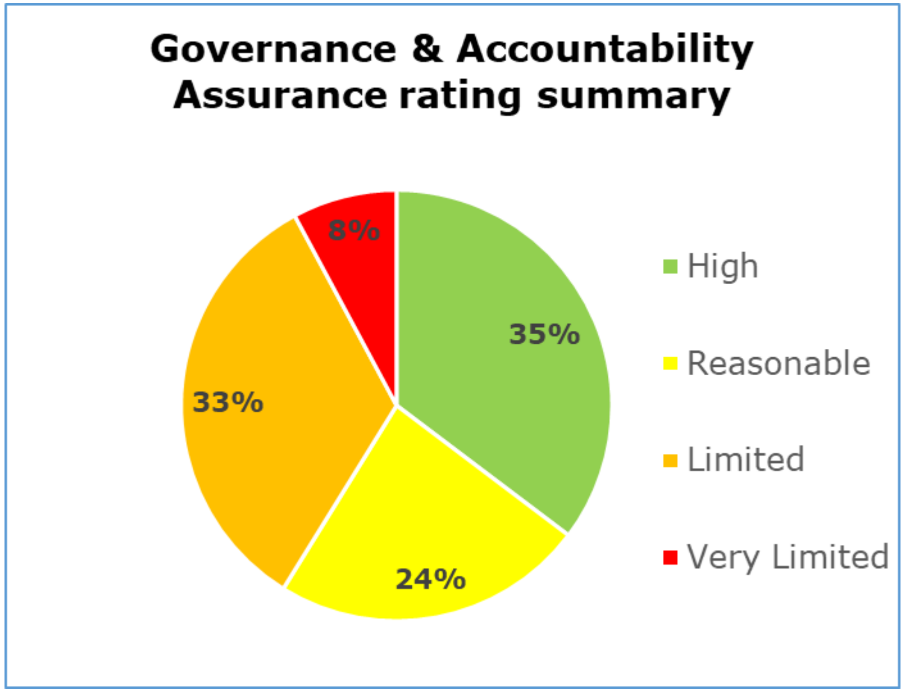
Priority Recommendations



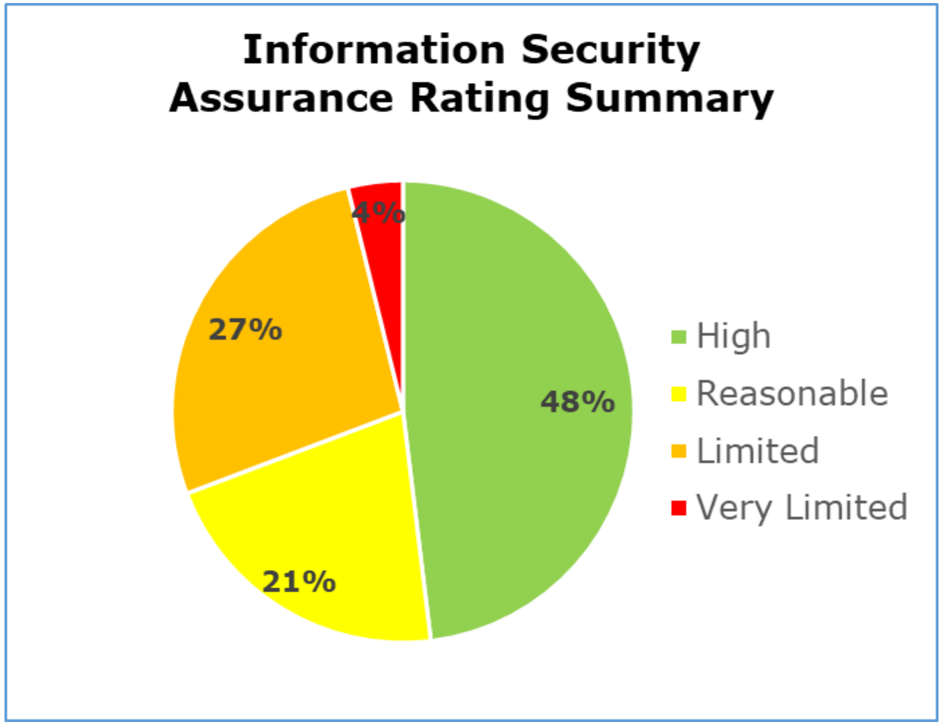
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has 3 urgent, 16 high, 10 medium and 4 low priority recommendations.
- Information Security has 14 high, 9 medium and 4 low priority recommendations.

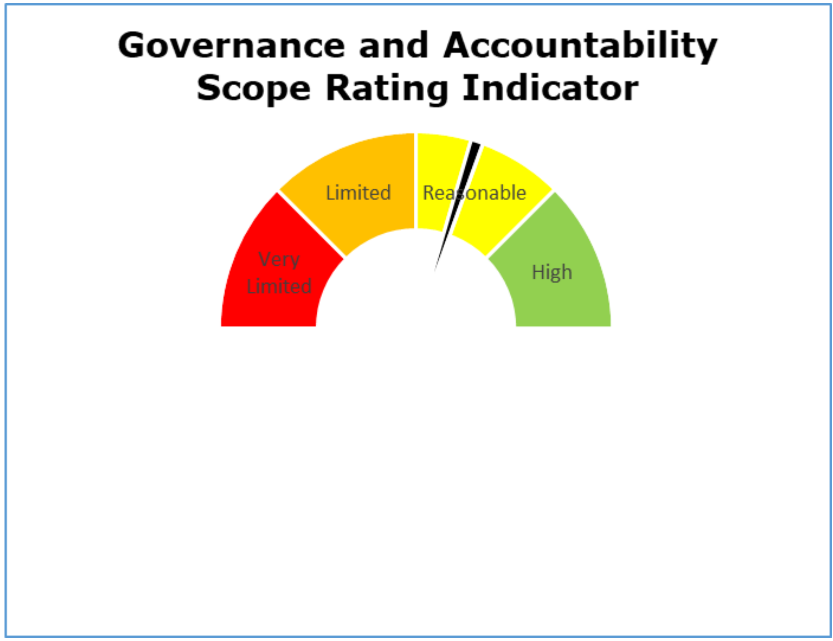
Graphs and Charts



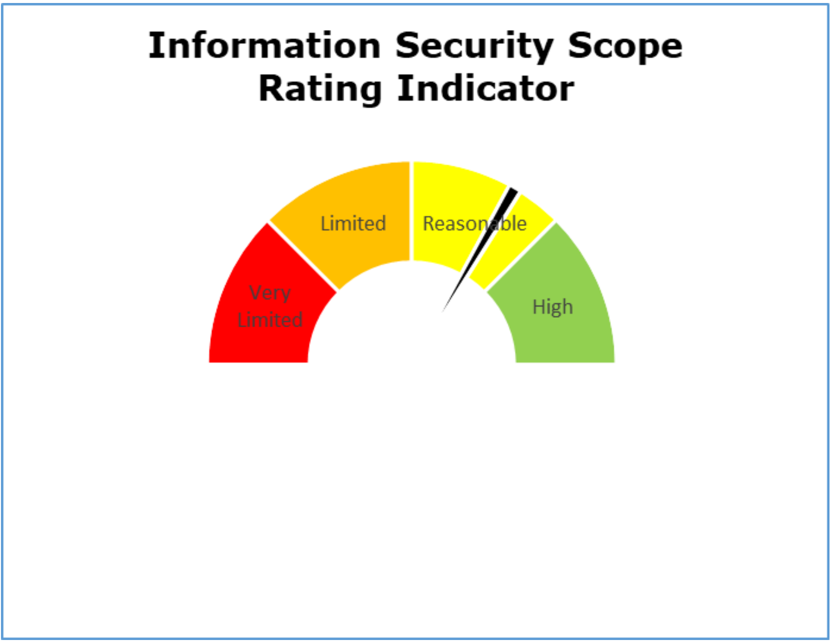
The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 35% high assurance, 24% reasonable assurance, 33% limited assurance, 8% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Information Security scope. 48% high assurance, 21% reasonable assurance, 27% limited assurance, 4% very limited assurance.



Governance and Accountability Scope Rating Indicator



Information Security Scope Rating Indicator

The speedometer charts above give a gauge of where the LAA sits on our assurance rating scale from high assurance to very limited assurance.

Areas for Improvement

The LAA should:

Ensure that defined risk management processes are in place so that de-escalated information risks are managed and recorded appropriately.

Complete a training needs analysis for all staff involved in the processing of personal data and roll out a suitable training programme to supplement the existing RFI e-learning. This training should be refreshed on a regular basis.

Complete the ongoing review of information assets and ensure that data flow mapping takes place to identify all processing activities that are not currently captured on the Record of Processing Activities (ROPA) or Information Asset Register (IAR). This should include information held on local drives as well as databases and systems. This should include identifying and recording the lawful basis for processing, and Schedule 1 condition where appropriate, for existing processing activities.

Implement a regular review of access controls, including privileged access rights, across all systems used by the LAA. This should include continuing with the Joiners, Movers, Leaver's project, particularly focusing on reviewing digital and physical access where staff move roles.

Identify IT systems that do not have effective logging or monitoring capabilities and implement an effective logging solution. When logs are in place, a programme of work to proactively review the content of the logs for misuse or suspicious activity should be established.

Establish and document controls around the use of social media, such as WhatsApp, for work related tasks including the sharing of personal information. The policy should be communicated to staff with checks on compliance proportionate to the risk.

Best Practice

The One Trust system is a DP compliance tool used across the whole of the MOJ to manage their ROPA, IARs and DPIAs. The use of the One Trust System to undertake DPIA screening and completion ensures a consistent way of gathering required information and allows centralised oversight of the DPIA process by the DPO and provides assurance to the MOJ. The different modules interact and information from DPIAs can feed into the ROPA to ensure that it is regularly updated. Once the tool is fully implemented it will allow the DPO Team to have oversight of all processing activity and information risk management in one system.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of the Legal Aid Agency.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of the Legal Aid Agency. The scope areas and controls covered by the audit have been tailored to the Legal Aid Agency and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.