Business Continuity Effectiveness Review

Information Commissioner's Office

March 2021

mazars

Contents

Business Continuity Effectiveness Review
Engagement objectives

01   To evaluate the effectiveness of the ICO's response to COVID-19, including a review of the lessons learnt and how these have been factored into its future continuity strategy and plans.

02   To assess the considerations the ICO have made against the approach similar sized organisations have taken to ensure they have put in place all the necessary measures to safeguard themselves in the future.

03   Determine how effective the ICO's response to the COVID-19 pandemic has been in terms of future proofing their continuity strategy and plans.

04   Produce a report of findings with a list of key considerations for ICO. These will be based on a combination of our expertise and the positive learnings that other organisations have implemented during the past ten months.

Business Continuity Effectiveness Review
Background

The ICO identified the possible threat of Covid-19 in January 2020 as worrying reports were being noted out of Wuhan, China. In response to this, the Head of Risk and Governance proposed the existence of a Coronavirus Working Group (CWG). The CWG was created outside of the proposed Business Continuity Plan's governance structure to operate as a pre-cursor group.

In March, the ICO invoked its Business Continuity Plan (BCP) and set up its Gold (strategic) Business Continuity Team (BCT) and Silver (operational/tactical) Incident Response Teams (IRT).

The BCT and IRT were able to react quickly to the events that unfolded in March, taking advantage of the planning and 'war-gaming' performed by the CWG. The CWG had already considered items such as capacity planning (resource and IT), requirements to work from home and how to manage an event whereby an employee caught Coronavirus.

The BCT and IRT teams managed the ICO response to Coronavirus from March to May before winding down these teams as the organisation had managed the initial 'emergency' response and moved towards a recovery phase.

In the lead up to the recovery phase, an internal lessons learnt exercise was held by the BCT and IRT to determine possible improvements to their response and business continuity planning more general. Upon completion of the lessons learnt exercise, the findings were passed to the Operation Volta programme team to incorporate into its programme of work, one strand of which was continuity planning with input from the Risk & Corporate Governance team.

Currently, the Risk & Corporate Governance team have produced, in conjunction with the relevant departments, departmental recovery plans which will eventually feed into the over-arching umbrella of the updated organisational BCP and the related business continuity policy statement.

# Business Continuity Effectiveness Review
Executive summary

Overall, it was felt that the ICO responded well to the Covid-19 pandemic with a quick return to a BAU governance structure. While the overall response was positive, the BCP that underpins the initial response to an emergency has room for improvement. We have outlined below what we believe are the key areas for the ICO to consider incorporating into its organisational BCP in response to future emergencies:

- **Communication strategy within the BCP** – the existing BCP does not provide sufficient detail to constitute a 'strategy'. It currently provides an outline of possible communication channels. While the identification of these channels is important, it should also be supported by a list of key stakeholders requiring communication, what they would need to be informed of, and the frequency of this communication.

- **Limited clarity on response actions by emergency type** – the information held in the current BCP does not provide clarity to the BCT as to who would perform the necessary actions outlined against each scenario, nor is there any obvious prioritisation attached against each item.
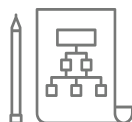
- **Identification of key themes within departmental plans** – the existing BCP has limited detail on the key cross-departmental activities/people/processes/systems that should be listed to perform a quick impact assessment when the nature and reach of an emergency is identified, enabling focus on actions to resolve any threat to key areas. This detail appears to be identified within the departmental plans and should therefore be aggregated up into the organisational BCP.

There is an opportunity to incorporate the above considerations, including our other findings into the to-be organisational BCP to enable it to be a reference document rather than a contact list which was also captured as feedback during the lessons learnt exercise undertaken by the ICO.

Business Continuity Effectiveness Review
Good practice overview

The overarching feedback from the key stakeholders interviewed has been largely positive, with particular focus on the overall management of the response to the first wave of Coronavirus and the speed at which the organisation was able to return to BAU governance structures, in most areas. We have noted elements of good practice within the ICO's response and have summarised the key themes below:

- **Coronavirus Working Group** – the CWG was in operation for approximately two months as a dedicated early-warning and planning team prior to the national lockdown. This enabled the ICO to get a head-start on its response to the Coronavirus, relative to other organisations. The CWG was extremely useful in exploring items such as IT capability, home-working planning and Coronavirus cases within the organisation ahead of time. Other organisations in comparison were often behind the curve and often found themselves setting up their BCT at the same time as trying to plan and respond to the pandemic in March.

- **Early return to BAU governance structures** – within three months of operation, the BCT and IRT were stood down and arrangements to transfer back to BAU governance structures took place, with Operation Volta taking on on-going responsibility for any critical incidents in response to Coronavirus. Other organisations are still in the process of standing down their respective Coronavirus response teams and are facing the struggle of reverting to new BAU governance structures whilst managing the on-going risk of Coronavirus.

- **On-going business continuity risk monitoring** – the ICO appears to be taking reasonable steps to future-proof itself from a business continuity risk perspective as there is regular business continuity reporting to the Risk & Governance Board. The risk management is underpinned by a three lines of defence approach as set out in the Business Continuity Policy Statement and Strategy document.

- **Departmental recovery plans** – ICO have created departmental recovery plans which take into account the detailed requirements of the entire organisation, rather than just an organisational wide BCP. This aids the individual departments in their recovery as well as directing the BCT and IRT in their actions. This is line with good practice that we have seen at other organisations as these are implemented in conjunction with the overall plan.

- **Cross team membership** – multiple stakeholders noted that the presence of the Head of Risk & Governance on both the Gold and Silver teams aided communication between the groups. The particular benefits noted were providing the rationale for decisions to Silver, while being able to provide Gold with additional operational context to make the decision.

Business Continuity Effectiveness Review
Observations & lessons learnt

ico.
Information Commissioner's Office

We have outlined below the findings of our review, these are contextualised by a comparison to other organisations to assist in the identification of good practice. Each group of recommendations is accompanied by an 'impact' rating which is a relative ranking of the recommendations noted to assist in the prioritisation of improvement opportunities. It does not correlate to any kind of risk rating that may be used by the Mazars Internal Audit team. We note that management intend to complete all recommendations by the end of the 2021 calendar year.

Observation	Comparison to other organisations	Recommendation	Impact	Management Response
Limited detail in the communication strategy – the communications strategy set out in section 4.2 of the current BCP is more of a guide than a strategy. It outlines the possible channels for communicating to parties during an emergency with brief guidance on how to utilise each. Communication was one of the recurring areas for improvement in the lessons learnt exercise.	One of the better communication strategies we have seen in a BCP outlines the key comms activities, the channels capable of mass communication to staff, pre-prepared public statements, key parties who may need to be communicated to and who in the organisation is responsible for making that contact, including general principles for all staff regarding communications to the press. This ensures consistent and timely communications to necessary parties.	• Develop this section of the BCP to incorporate elements from those shown under the 'comparison to other organisations' section. We would anticipate the comms strategy to include the who (recipient), what (content), how (channel) and when (frequency) as a minimum. • Ensure the communication sections in each departmental recovery plan are aggregated into the organisational BCP as appropriate.	1 2 3 4 **5**	Agreed as suggested for both bullet points and will update BCP to reflect this.
Ensure key elements of departmental BCPs are captured in the Corporate BCP – consider the overall responses within each section of the April 2020 plans to identify key elements. For example, key interdependencies (e.g. where large number of departments rely on the same element) should be aggregated to enable the assessment of the possible impact of a future emergency. The existing BCP only appears to cover 'Key Work Priorities', however it is hard to quickly identify how these may be affected by a given emergency.	Some BCPs in other organisations have noted at a high level the key elements of their organisation and the key dependencies for the minimum possible operation of these. This enables a rapid assessment of the possible impact of an emergency on the organisation's key areas (people, systems, processes etc).	• Identify the key systems/people dependencies in the ICO for it to continue operating effectively in the event of an emergency.	1 2 3 4 **5**	Whilst this is covered in some part by the high level business impact assessment this isn't presently referred to in the Corporate BCP. As suggested we will include or at least link to the key systems and people and ensure these tally with the departmental BCPs

Observations & lessons learnt

ico.
Information Commissioner's Office

Observation	Comparison to other organisations	Recommendation	Impact	Management Response
Detail of possible impact scenarios and actions – the information held in section 3.4 of the current BCP does not provide clarity to the BCT as to who would perform the actions outlined in each scenario, nor is there any obvious prioritisation attached to each item.	Some BCPs produced by other organisations use one page flow-charts to set out a standard response to possible emergency scenarios. Each sets out a high-level flow of actions to be taken that refer to defined emergency procedures held in the appendices (e.g. evacuation, mass communication to staff etc.). It also assigns responsibility for actions to high level groups, i.e. EMT, Recovery Team and dependent groups (e.g. intruder alert includes actions for the Security team), for example.	• Review the level of detail that is provided in section 3.4 and how this will be reflected in the new organisational BCP. During the lessons learnt exercise it was noted that the BCP was not used as a reference document, therefore the inclusion of detail such as this would enable the ICO to act quicker and with greater assurance it is addressing the 'correct' areas.	[1 2 3 4 **5**]	We will review and include a high level flow of actions for corporate scenarios as suggested. We will also include a decision matrix to aid decision making for implementation of departmental level BC plans.
There is no formal Terms of Reference for the Gold & Silver Teams – we have noted that the transition from CWG to Gold and Silver Teams was supported by a high level handover note. We also note that the BCP sets out a very high-level focus for these two teams. A formal ToR was not produced to support and outline the roles & responsibilities of the teams, including remit relative to other governance groups in the organisation. This would likely resolve the lesson regarding the confusion in the roles and membership of Gold & Silver teams.	Similarly, most organisations did not produce a formal ToR to outline the responsibilities of their BCT. We have noted that in the organisations that did operate a formal ToR, they tended to have a better overall organisational response to the pandemic.	• Produce formal ToRs to accompany any governance groups that are created. • It is likely that the remit of the Gold and Silver teams will have the same over-arching principles regardless of the pandemic type. These could be detailed in the BCP to provide a starting point before the creation of more detailed ToRs once the nature of an emergency is clearer.	[1 2 3 **4** 5]	We will include 'draft' ToRs as an appendix to the corporate BCP to help inform and formalise any governance groups created in future.
Optional sign-up to text service – staff are currently able to opt out of the text service.	Most of the organisations we have worked with recognise the importance of an all staff text service as the most simple and direct means of providing basic, important communication to all staff. The ease of use and tracking provides assurance that important messages are received.	• Review the current policy and look to make it mandatory.	[1 2 3 **4** 5]	We will review the current policy and seek to encourage staff to opt in but as this includes personal phone numbers it is likely that this would be staff preference.

Business Continuity Effectiveness Review
Observations & lessons learnt

ico.
Information Commissioner's Office

Observation	Comparison to other organisations	Recommendation	Impact	Management Response
There are no deputy individuals identified within the current BCP – should some members of the BCT or in other senior/key roles become unavailable, there is no obvious succession planning in the BCP. We note that deputies have been identified for 'Key Work Priorities' but this does not appear to have been applied elsewhere. This is important for the ICO as anecdotal evidence suggests that the ICO was reliant on some individuals during the initial response to the Coronavirus pandemic due to their organisational knowledge and position.	A lot of the organisations we have performed similar reviews for have identified the key individuals and/or roles within SMTs and the BCT outlines who might take over in the short/long-term should such key people become unavailable.	• Identify key roles, beyond purely a process viewpoint, within the organisation and the BCT and assign a deputy to each.	`1` `2` `3` `4` `5`	Agreed with recommendation made and will update the BCP to include this.
Inconsistent cascading of information from managers – anecdotal evidence suggests that some managers were not as effective at cascading information as others, stakeholders noted that this was more likely due to the format of how information was provided rather than a lack of information. **Managers passed issues up the chain unnecessarily** – similarly, some managers were referring questions and issues upwards as they were unsure of the response required.	In other organisations that performed well at cascading information, they provided managers with an overview of the information to be cascaded and followed this up with drop-in sessions where managers could clarify points to relay it to staff. Good organisations also tried to maintain a consistent frequency of information provision, as far as government guidance allowed. It should be noted that inconsistent cascading of information by managers has been noted in almost every review we have performed.	• Develop methods for supporting managers with the information to be cascaded – we have noted the following to work in other organisations: manager drop-in sessions before and after communications, and summaries of key points alongside the detailed document. Where required, drafting comms for managers has been noted to provide consistency. • Where possible, utilise a communication log and plan to schedule information provisions.	`1` `2` `3` `4` `5`	Agreed with recommendations made and will note a help prompt within the BCP. A communication log template will be included as an appendix template.

Business Continuity Effectiveness Review
Observations & lessons learnt

ico.
Information Commissioner's Office

Observation	Comparison to other organisations	Recommendation	Impact	Management Response
Possible duplication of effort – due to the nature of Operation Volta's aims and how they manifest themselves in BAU activity, there is a risk that some activities and governance elements may overlap with those on the departmental BAU side.	A lot of organisations have struggled to separate their on-going business continuity response, the recovery works and BAU activities and governance structures from each other.	• As the Project Volta ToR is updated in the near-future, take this opportunity to review deliverables and governance structures between Volta and BAU to ensure there is no duplication of effort and similarly, no gaps.	1 2 3 **4** 5	Agreed – this is part of Volta's action plan and is already in train.
Possible friction between Gold & Silver teams – it was noted that some members of the CWG would later become part of the Silver team who were primarily charged with carrying out decisions made for them by the Gold team. This is a paradigm shift for these members, both groups need to be clear on the shift in responsibilities to ensure all are pulling in the same direction.	In other organisations that had groups set up prior to invoking their Business Continuity Plans, these tended to be very senior figures that sat on the top-tier of their Business Continuity governance structures.	• Carefully consider the membership of groups that are created outside of typical governance structures considering how these may change as the situation evolves.	1 2 **3** 4 5	Agreed. A short note to this effect will be included within the overarching BCP and in the 'draft' ToR for the groups.

Appendix

mazars

ico.

Stakeholders interviewed & documents provided

ico.
Information Commissioner's Office

Stakeholders interviewed

- Jennifer Green - Director of Communications and Programme Sponsor for Operation Volta

- Mike Fitzgerald, Director of Digital, IT and Business Services

- Suzanne Gordon, Director of Public Advice and Data Protection Complaints

- Louise Byers, Director of Risk and Corporate Governance

- Joanne Butler, Head of Risk & Governance

- Peter Bloomfield, Operation Volta Programme Manager

Documents provided

- 202003 Dept BC Covid 19 Plan Digital & IT

- 202004 Dept BC Covid 19 Plan Investigations Update

- 202007 Dept BC Recovery Plan Finance & Procurement

- 202007 Dept BC Recovery Plan PGA

- 202008 Dept BC Plan Various Scenarios Business Services

- 202008 Dept BC Plan Various Scenarios Legal Enf

- 20190718 Business Continuity Plan Team Version - updated 20200316

- 20200609 PB Doc 4.0 Lessons learnt paper

- 20210121 Volta ToR

- Audit Committee - VOLTA v1

- Audit Committee BC Policy

- Business Continuity Policy Statement and Strategy

- HR and Facilities BIA - post peer review

- July 2020 Staff Wellbeing Survey - you said we did

- Lessons Learned Questions

- Policy Legal BIA

- TOR 20200507 Operation VOLTA

mazars

Contact

Mazars

Catrin Davies

Manager, Business Consulting

Catrin.Davies@mazars.co.uk

Kieran Higgins

Senior Consultant, Business Consulting

Kieran.Higgins@mazars.co.uk

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of 40,400 professionals – 24,400 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*where permitted under applicable country laws.

www.mazars.com

mazars

ico.
Information Commissioner's Office