Meeting	Executive Team	**Date**	Monday 24 September
Paper title	Business Continuity Plan Review - Mission Critical Activities		
Agenda item	5	**Discussion time**	15 minutes
Purpose of paper [If a "decision" you must complete the template overleaf]	Decision		
Restrictions on public access including staff	Restrictions?		N
	If "Y" please give the reason for the restriction below.		
Presenter	Lesley Bett and Jolyon Stone		
ET sponsor	Daniel Benjamin		
Corporate Plan aim	7.9 – continue to review and improve the ICO's corporate governance and its own compliance with information rights legislation.		
Summary	Agree the ICO critical services and activities identified by the Business Impact Analysis and business continuity plan review working group.		
Who has been consulted? [eg staff, stakeholders, trade unions]	Heads of Departments, Director of Corporate Services, Assistant Commissioner (Scotland & Northern Ireland), Assistant Commissioner (Wales), and ICO BCP working group.		

Business Continuity Plan Review – Mission Critical Activities

Introduction / Aim of the paper

1. ICO's Business Continuity Plan (BCP) is being reviewed following an internal audit. The starting point for business continuity planning is to identify the organisation's mission critical activities (MCAs). The MCAs are those ICO activities which would be the focus of **immediate attention** if the business continuity plan is invoked.

2. One of the recommendations from the internal audit is that ET should re-evaluate the ICO's mission critical activities (MCAs) based on its mission and vision, stakeholder obligations and statutory duties. The business continuity working group has carried out some work in this area and the purpose of this paper is to recommend a revised list of MCAs for discussion and agreement.

Decisions needed and recommendations made

3. To agree that the key services underpinned by critical infrastructure activities referenced in Annex A are to be regarded as mission critical. If they are agreed, the business continuity plan will set out the practical arrangements to achieve priority recovery of these key services and infrastructure. A second phase of planning would achieve the recovery of remaining services.

Background

4. Following an internal audit of the ICO's Business Continuity Plan a working group was set up to action the recommendations. In the main, the recommendations were concerned with the need to review the existing plan including:
    - reconsidering the identified key services and critical activities and the resources required to support them
    - re-evaluating the threats to the key services and critical activities
    - reviewing the plans to mitigate against those threats and recover from an incident should a threat materialise.

5. A business impact analysis (BIA) was conducted to re-evaluate the ICO's key services and critical activities. The BIA involved Heads of Departments reviewing ICO services in their area of responsibility, the IT systems and departments they are reliant upon and the likely impact on the ICO if each service were to fail following an incident.

6. The first stage of the BIA recorded the impact on the ICO both in terms of the reputational damage and its statutory obligations as well as estimating the recovery time for each service.

7. The second stage of the BIA involved interviewing Heads of Departments responsible for services identified as having a high impact, both in terms of reputational damage and statutory obligations on the ICO if they were to fail. For each service the identified minimum staffing levels and skills required were identified and the maximum tolerable period of disruption determined.

8. The working group discussed the high impact services and activities identified from the BIA and agreed the list of ICO key services and critical infrastructure activities to be recommended to ET and to be included in the revised BCP. The list is short and focuses on the essential services and infrastructure activities to be prioritised in the first two weeks following an incident. Plans would be developed to recover the remaining services after the MCAs have been addressed.

9. The MCAs should be seen as a checklist for the Executive Team in the event of an incident.

<u>Options considered</u>

10. All ICO services were reviewed by Heads of Departments and findings were fed into impact matrices that were used to rank services in order of criticality.

<u>Risks and opportunities</u>

11. The risks are that, in the event of an incident, key ICO services will not be recovered in time to mitigate against both the reputational damage and failure to carry out our statutory duties as a regulator and employer.

12. The proposed ICO key services and critical infrastructure activities provide an opportunity for the Executive Team, Heads of departments and managers to consider where resources are best placed, in the event of an incident.

<u>Financial issues</u>

13. There are no financial issues identified.

<u>Staffing issues</u>

14. Awareness raising of business continuity plans and procedures to enable staff and managers to act accordingly in the event of an incident.

Devolved office issues

15. The review of the business continuity plan includes BCP arrangements for the devolved offices.

Privacy issues

16. It was agreed that the security of information would be a critical infrastructure activity that should be addressed immediately in the event of an incident and during recovery of ICO services.

Conclusion

17. Correct identification of MCAs is an essential part of business continuity planning. Well understood priorities and effective practical arrangements to address them should ensure a prompt start on recovery. If the number of MCAs is too high there is a danger that effort and resources could be spread too thinly and slow down recovery.

Annexes

Annex A - details the current MCAs listed in the Business Continuity Plan and the proposed key services and infrastructure activities for the revised plan.

Annex B - is the summary of high impact services/activities as recorded in the business impact analysis

Annex A

Existing MCAs in the current ICO BCP (February 2012)

Primary MCA’s

1. Communications (social media, staff, website and press office)
2. Obtaining funds and accessing them/Cash Flow and Paying Staff
3. Maintaining site security and safety
4. Maintaining an acceptable level of IT

Secondary MCA’s

1. Dealing with enquiries (customer contact and notification help lines/written enquiries)
2. Internal Compliance (Information requests and requests for internal review)
3. Producing the statement of account & the annual report
4. Dealing with complaints
5. Maintaining a register of data controllers.

Proposed ICO key services and critical infrastructure activities

ICO Key Services

- Obtaining funds and accessing them (ability to pay suppliers/staff, receive and bank notification fees)
- Communication to external stakeholders (maintaining and updating the website, press office, limited helpline facility)
- Current/on-going investigations, prosecutions, appeals
- Current/on-going ICO policy and stakeholder liaison (e.g. attendance at Select Committees and contributions to consultations)

ICO Critical Infrastructure Activities

- Safety of staff and security of information/site
- Internal Communications
- Recovering/maintaining IT systems and facilities

One of the main differences is that the proposed list of MCAs is much shorter and has focused on those services and activities which are considered to be essential in the immediate aftermath of a serious incident and specifically to be addressed in the **first two weeks** of recovery. Much of the emphasis would be on communications both externally to inform stakeholders of our position and plans and internally with our staff to ensure they are kept informed and understand what they need to do. IT and accommodation issues would need to be addressed before most operational services could be recovered.

The proposed list also reflects the need to consider any high impact, high profile activities and events ICO may be working on at the time of the incident.

Services such as dealing with enquiries/complaints, information requests and producing the statement of accounts and the annual report have been removed from the proposed list. The recovery of these services are dependent on the successful completion of the identified MCAs.