Audit and Risk Committee – for assurance

Meeting agenda title: Business Continuity Management Policy Statement

Meeting date: 10 January 2022

Time required: 15 minutes

Presenter: Joanne Butler

Approved by: Louise Byers

1. Objective and recommendation

1.1. The purpose of this report is to give the Committee assurance on the development of the ICO's business continuity practices, in the contextof the Business Continuity Management Policy. The Committee is recommended to comment on and note the report.

2. History and dependencies

2.1. The Committee received v1.0 of the ICO's Business Continuity Management Policy Statement at its January 2021 meeting and requested that it receive annual updates on business continuity.

3. Developing a common understanding

3.1. The purpose of the Business Continuity Management Policy Statement is to set out the ICO's overall approach to business continuity. This policy statement is supported by the Business Continuity Plan, which sets out how the ICO will respond to business continuity incidents.

4. Matters to consider to achieve objective

4.1. We have reviewed the policy and it remains fit for purposes. Therefore, only minor changes have been made to the policy. The updated policy is at Annex 1. The minor changes in the policy bely the amount of focus that has been put on this area, particularly over the last six months, with the Risk and Governance Team reviewing the Business Continuity Plan.

4.2. For example, the minor amendment to the policy of saying that we will have Gold, Silver and Bronze response teams (rather than just Gold and Silver teams) is a fundamental change in our business continuity approach. We have also developed terms of reference for the Gold and Silver teams to ensure that there is clarity about the roles of each of these teams.

4.3. We have also added further information into the Business Continuity Plan about issues to consider in deciding whether to invoke business continuity, further information about communications activities to ensure that there is clarity about this crucial part of the business contiuity response, and identified priority activities, staff requirements, dependencies and essential suppliers. This has all been informed by the lessons learned from the response to the COVID-19 pandemic, as well as the recommendations from an advisory audit by Mazars earlier in the year. All of the recommendations from that advisory audit have been implemented.

4.4. Looking forward, we are in the process of reviewing the incident response plans for various different types of business continuity incidents, which will increase the maturity and preparedness of the organisation if there is such a business continuity event. We currently have three types of incident response plan (staff unavailability, premises unavailability, IT unavailability), but are expanding that to provide more nuance. The incident response plans that we are developing are:

- Significant Staff absence
- Premises unavailability
- Cyber security incident
- Ransomware incident
- Widespread IT systems outage
- Terrorist incident anywhere where ICO staff may be (we currently have a brief section of the plan which sets this out, but it will be expanded).

4.5. Each of these incident response plans will include actions for all relevant areas (e.g. an IT outage plan will include actions for IT, facilities, communications, corporate governance, HR and so on).

4.6. During 2022 we will run exercises to test some of these incident response plans, beginning with a desktop test of the draft ransomware response plan early in the year.

4.7. The key challenge throughout the year on business continuity has been resources. To this end, we will be recruiting a Risk and

Business Continuity Manager in early 2022. Their role will be to continue the development of our business continuity maturity, particularly including organising and running the further desktop testing exercises.

5. Areas for challenge

5.1. Are the objective the policy set out still the right business continuity objectives for the organisation? Does the policy continue to set the right level of ambition?

5.2. Is the level of progress with the business continuiuty plan appropriate?

6. Communications considerations

6.1. There are no communications considerations for this report at this time.

7. Next steps

7.1. The next steps for this work are:

- Complete the review of the business continuity plan.
- Complete the development of the revised incident response plans.
- Deliver desktop exercises for the incident response plans, starting with ransomware.

Author: Chris Braithwaite

Consultees: Louise Byers, Joanne Butler

List of Annexes: Annex 1 – Business Continuity Management Policy Statement, v1.1 (draft)

Publication decision: This report can be published internally and externally without redaction.

Outcome reached: