Human
Fertilisation &
Embryology
Authority

Business Continuity, Resilience and Cyber Security

Strategic delivery:	☒ Setting standards	☐ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item	8		
Paper number	AGC (03/10/2017) 564 DH		
Meeting date	03 October 2017		
Author	Dan Howard, Chief Information Officer		
Output:			
For information or decision?	For information		
Recommendation	The Committee is asked to Note: • Progress and headline results relating to the Business Continuity Test undertaken in September 2017 • Details of the BCP 'tabletop' test due to take place shortly • The 'Impact on Members section' regarding BCP awareness • Details of the Office 365 security safeguards which are in place • Headline information from the Cyber Security component of the IT work programme		
Resource implications	None		
Implementation date	During 2017–18 business year		
Communication(s)	Regular, range of mechanisms		
Organisational risk	☐ Low	☒ Medium	☐ High
Annexes:	None		

1. Background

1.1. This paper provides an update on our arrangements for business continuity, for preparing and managing our activity in the event of loss of staff, information technology support, or office accommodation. This paper provides details of improvements that have recently been made along with the results of associated testing.

1.2. This paper also provides an update on resilience and cyber security and contains an update on key aspects of the associated work programme. This will be continually developed and reviewed to address actual and perceived threats associated to our data, infrastructure and technology landscape.

2. Introduction

2.1. In June 2017, AGC received an update on Business Continuity Planning. The update included details of future arrangements including a communications exercise, configuration of our BCP 'landing page' within O365 Sharepoint, a refresh of contact information and the integration of Members within our BCP arrangements. This work is now nearing completion and this paper provides a further update on progress.

2.2. We are developing our work programme. This programme will include elements relating to cyber security. Further details will be available as the programme is confirmed.

3. Business Continuity Testing

3.1. Following the BCP update reported to AGC in June 2017, several improvements have been made. These include:

- **Communication:** User guidance for accessing our BCP site within Sharepoint was revised and forwarded to all staff. Staff were given instructions for accessing via different device types. Staff were encouraged to test out access and feedback was invited. Support was made available to anyone who did not feel confident accessing the site;
- **BCP 'landing page':** Minor amendments were made to the structure and content of the page. To encourage all activity to remain on the BCP page, the link to Yammer (Collaboration social network tool) was also removed;
- **Contact information:** As part of the BCP awareness campaign, staff were encouraged to update their contact details – namely the mobile telephone number to be used in the event of the BCP being invoked; and,
- **Integration of Members in Business Continuity Planning:** Rather than require an immediate response from Authority Members as part of the main BCP test, it was agreed that the focus would be on awareness and testing access to the BCP site by Members. This work is ongoing and is expected to be concluded ahead of the meeting.

3.2. During the week commencing 18th September 2017, we tested our Business Continuity Plan. Staff were informed that a BCP test was likely to take place but not given details of timescales.

- The test involved sending a text message to the mobile telephone number on record and requesting they a) access our BCP site and b) to follow further instructions on arrival.
- A test message was sent out at 7.07pm on Wednesday 20 September. The first message notified staff that the test was taking place and contained details of the BCP site weblink. A second message contained further information on the format of username to use.
- The test was largely successful. Around 60% of staff accessed the site within the first four hours and added a comment to the comments section. This rose to around 90% of staff accessing the page during the following working day. Staff on leave or otherwise absent from work are excluded from these totals. It should be recognised that this was a test and evidence suggests access rates in a real BCP situation are typically higher. Staff who did not access within the timeframe above were contacted to provide support to ensure they are able to access the site if required in the future.

3.3. The BCP test above can only test one scenario and so to further strengthen our controls, we will be undertaking a ‘tabletop’ BCP test on 27 September 2017. This will involve simulating several scenarios. Participants will have no knowledge of details ahead of the session. An oral update on results and lessons learned will be provided to the Committee.

4. Cyber Security

4.1. Our cyber security controls (such as technology, processes and practices – for example firewalls, access controls and user access) remain under review and improvements will be made as necessary to address actual or perceived risk.

4.2. Our work programme includes associated awareness training for staff and our target is all staff will have completed necessary training within the previous 12 months by the end of the 2017 calendar year. Our work programme includes a strand to move our remaining data and infrastructure into the Microsoft cloud.

5. Impact on Members

5.1. We recognise that our BCP testing must include Members’ readiness. Following the all-staff test we now plan to invite feedback from Authority Members. Guidance will be forwarded during the week commencing 25 September requesting the BCP site is accessed and an oral update will be provided to the Committee.

5.2. Assurance has been sought on the security safeguards in place within Office 365. As standard, these include built in anti-virus and anti-spam. They also include protection from incoming threats e.g. viruses from machines used to connect to the Office 365 environment when it is accessed through the Office 365 website.

5.3. There are significant additional controls in place which include physical (access to datacentres such as personnel), logical (processes used to minimise risks to data, such as anticipating malicious access) and security (such as the technical encryption of all data while in use). For further assurance Microsoft comply with the ISO 27018 Code of Practice for Protecting for Protecting Personal Data in the Cloud. They were the first Cloud provider to do so.

5.4. To follow good practice, Authority Members are reminded that they should install anti-virus software on personal devices and ensure it remains up to date.

6. Risks and issues

6.1. While the access rate following the BCP site was encouraging, feedback suggested that access from a smartphone was difficult as the page was not easy to navigate. To address these concerns, we have updated the page layout to make it easier to use.

7. Recommendation

The Committee is asked to note:

- Progress and headline results relating to the Business Continuity Test undertaken in September 2017
- Details of the BCP 'tabletop' test due to take place shortly
- BCP awareness within the Impact on Members section within this paper
- Details of the Office 365 security safeguards which are in place
- Headline information from the Cyber Security component of the IT work programme