Resilience, Business Continuity Management and Cyber Security

Strategic delivery:	☒ Setting standards	☐ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item	10		
Paper number	AGC (05/12/2017) 580 DH		
Meeting date	05 December 2017		
Author	Dan Howard, Chief Information Officer		
Output:			
For information or decision?	For information		
Recommendation	The Committee is asked to note: • This update including progress made relating to BC testing, our BCP and the management of Cyber Security risk • That Resilience, Business Continuity Management and Cyber Security issues will be escalated as appropriate and AGC will be kept abreast of any developments where necessary		
Resource implications	None		
Implementation date	Ongoing		
Communication(s)	Regular, range of mechanisms		
Organisational risk	☐ Low	☒ Medium	☐ High
Annexes:	None		

1. Background

1.1. In recent months, AGC have received regular and detailed updates on Resilience, Business Continuity Management and Cyber Security, along with updates relating to the completion of associated actions.

2. Progress update

2.1. Business Continuity testing has progressed well since the previous update in October 2017. Authority Members are able to access the BCP Sharepoint page within the Office 365 environment. Several have accessed this for testing purposes.

2.2. On 22 November 2017 CMG considered an updated Business Continuity Plan which includes all lessons learnt and feedback from the testing. Feedback has also been sought from the Authority Member responsible for Business Continuity. CMG carefully considered issues relating to the availability of systems/services and our business requirements.

2.3. Cyber security risks are continually monitored and escalated where necessary. We manage risk through a variety of methods, including reviewing and actioning weekly CareCERT Cyber Security Bulletins issued by NHS Digital.

2.4. Cyber security training is mandatory and the next refresh will require all staff to complete the 'Responsible for information: general user' course before the end of December 2017; the course is delivered through Civil Service eLearning

3. Recommendation

The Committee is asked to note:

- This update including progress made relating to BC testing, our BCP and the management of Cyber Security risk
- That Resilience, Business Continuity Management and Cyber Security issues will be escalated as appropriate and AGC will be kept abreast of any developments where necessary