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 (21/03/2017) 535 DM		
Meeting date	21 March 2017		
Author	David Moysen, Head of Information Technology		
Output:			
For information or decision?	For information		
Recommendation	The Committee is asked to note this report.		
Resource implications	No additional resources, costs incurred within IfQ programme or business as usual expenditure		
Implementation date	Ongoing		
Communication(s)	Ongoing		
Organisational risk	☐ Low	☒ Medium	☐ High
Annexes	• Health Group Internal Audit report – cloud cyber risk assessment • HFEA Clinic Portal penetration test assessment and recommendations		

1. Introduction and summary

1.1. Cybercrime is an increasing threat and the HFEA, like the rest of the public sector, is seeking elevated cyber defence strategies and assurance. The recent formation of the National Cyber Security Centre (NCSC) which has taken on and replaced the functions of CESG; the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI) underlines the Government's commitment to reduce cyber security risk nationally.

1.2. In line with this and HFEA's commitment to a cloud first strategy, the HFEA has been taking robust steps to ensure that the HFEA's systems are being developed in a secure way and hosted securely.

1.3. This paper sets out the steps we have taken most recently to ensure that our arrangements for cyber threat are robust and meet expected standards.

2. Cyber Cloud Risk Assessment

2.1. The HFEA operates in a predominantly 'cloud' based environment utilising an Azure service platform to provide the service platform necessary to run the business including achieving the goals of the IfQ programme.

2.2. Members will be aware of the internal audit draft on cyber cloud risk assessment undertaken recently.

2.3. This piece of work specifically relates to the risks that are inherent with moving to a cloud hosted paradigm and rates the overall hosting strategy as moderate with two low priority recommendations which have been accepted and are being actioned.

2.4. However, it is of note that the possibility of lock in with the Azure platform has a financial (as well as a security) dimension to be considered. The HFEA is committed to providing best value from its resources. Whilst there is no financial lock-in with Microsoft, we were conscious of the risks of over dependence on a single supplier in designing our approach. As such, our service can be moved to an alternative different vendor if there is a significant commercial advantage.

2.5. The report is appended.

3. IfQ risks

3.1. The IfQ programme, through the introduction of three distinct points of 'attack' is an area of considerable attention. At the outset of the programme we commissioned a *CLAS* consultant to sit alongside us for the duration of the programme.

3.2. The category of CLAS consultant was introduced by CESG (Comunications-Electronics security group - a part of GCHQ), the UK government's national technical authority for information assurance. It protects the UK by providing policy and assistance on the security of communications and electronic data, in partnership with industry and academia. A CLAS consultant is approved by CESG.

3.3. That said, the CLAS consultant category has now been replaced by the Certified Cyber Security Consultancy (CCSC) scheme – which differs mainly in the sense that consultancies rather than individual consultants are accredited. Our adviser is registered as such.

3.4. At the conclusion of the programme, on the basis that we have followed all necessary steps the SRO (Nick Jones) will receive documentation as to the security of the system (high) and the steps necessary to maintain an acceptable level of security.

3.5. In the meantime, we have adopted a robust approach to security testing (cyber or otherwise) for each of the principal IfQ products, as defined by the Clas consultant:

HFEA Clinic Portal

3.6. In advance of the IFQ Portal product going live (in January 2017), the HFEA commissioned external penetration testing from NTA Monitor. [This is in addition to the development phase penetration testing that AGC previously received.] The report listed 10 concerns and rated the overall solution at medium risk. Prior to the portal going live, 8 of the concerns highlighted were mitigated and the remaining two risks were accepted by the IFQ Programme Board. The report is appended.

IFQ Website

3.7. The Website product has just been though GDS go-live assessment and final penetration testing for this has been scheduled, in anticipation of success. This is the approach adopted for the launch of the clinic Portal; with testing taking place as close to the launch date as feasible.

IFQ EDI Replacement

3.8. Development continues and the HFEA has commissioned NTA Monitor to provide ongoing security advice during the build period and we are working with our external Clas consultant to provide assurance around the solution and to create suitable operational monitoring SOPs.

4. Recommendation:

4.1. The Audit and Governance Committee is asked to:

- Note the steps taken to ensure robust mechanisms for managing the cyber security threats are in place, and the assurance provided by internal audit and commissioned external experts

5. Annexes:

- Health Group Internal Audit report – cloud cyber risk assessment
- HFEA Clinic Portal penetration test assessment and recommendations

HFEA Clinic Portal Penetration Test Assessment and Recommendations

Overview

NTA Monitor performed penetration testing on the R1 portal product in the week commencing 3rd of January. The testing was performed against the Beta Portal Site and its' associated API and identified a number of vulnerabilities as listed in the table below. Overall the solution was assessed as being at a medium risk.

Assessment Number	Confirmed Severity	Ref.	Brief Description	Count
1	Medium	APP-882	Exposed CMS admin interface	1
2	Medium	ENC-424	TLS version 1.0 in use	1
3	Medium	ERH-942	Web applications allow virus files to be uploaded	1
4	Medium	API-141	API server supports plaintext basic authentication	1
5	Medium	API-837	No account lockout mechanism in place	1
6	Low	APP-068	Servers offer unknown network services	1
7	Low	SES-857	Session idle timeout too long	1
8	Low	SES-903	Secure page browser cache	1
9	Low	WEB-140	Web servers advertise software type and version	1
10	Low	WEB-165	Web servers leak ASP.NET version information	1

This document will address the individual concerns that have been made and mitigations that may be made against them. IFQ Programme Board is requested to review the following and to determine if the residual risk elements are acceptable for the Portal to go live.

Assessments

1 Exposed CMS admin interface

Administration of the Portal requires suitably privileged users to log in to a specific url on the portal. APP-882 raises the risk that as this is a well-known address, potential

attackers could use this information to expose any vulnerabilities that are present in the admin interface. The recommended solution is to allow access to this interface only from a known source address, in this case the HFEA offices. This would have the side effect of preventing content changes by remote workers unless the HFEA implements a specific remote access regime for those affected.

Programme Board is asked to decide whether to restrict access on this basis or not.

2 TLS version 1.0 in use

The azure web server components currently allow the use of a set of encryption technologies known as TLS 1.0 .ENC-424 acknowledges that vulnerabilities exist in these technologies and the current PCI guidelines mandate upgrading to TLS 1.2 or higher by June 2018. The encryption standards supported by the Azure web platform are controlled by Microsoft and it is anticipated that they will remove these standards by the above mentioned date.

Programme Board is asked to acknowledge this risk and its future mitigation.

3 Web applications allow virus files to be uploaded

The portal application allows virus files to be uploaded. ERH-942 reflects that the system will allow files containing viruses to be uploaded. This presupposes that a clinic end user has no antivirus software installed or is deliberately trying to upload a virus. The uploader only allows specific file types to be uploaded and, additionally, HFEA end users who attempt to access such an upload will have the content block by the antimalware systems installed locally. If required, the HFEA could implement a process by which uploaded material is scanned before being transferred into HFEA systems.

Programme Board is asked to acknowledge this risk and whether further mitigations should be applied.

4 API server supports plaintext basic authentication

APi-141 raises the risk that a simple authentication scheme is used at the API level. This is indeed true for the system presented for testing. However, this mechanism was specifically allowed to enable NTA access to the API for other testing and will not be deployed in production.

Programme Board is asked to acknowledge this risk has been mitigated.

5 No account lockout mechanism in place

API-837 raises the risk that user accounts used to authenticate against the API are not locked out after a number of failed attempts. As in 4 above, this vulnerability will not be present in production.

Programme Board is asked to acknowledge this risk has been mitigated.

6 Servers offer unknown network services

APP-068 reports that the servers hosting the Portal application offer unknown network services and recommends that these services be firewalled or disabled. The services detected are part of the configuration and management system that is used by the Azure environment and their security is managed by Microsoft.

Programme Board is asked to acknowledge that no action is required.

7 Session idle timeout too long

SES-857 reports that inactive user sessions are timed out after 30 minutes of activity and that best practice would be to remove inactive session after 5-10 minutes. The session timeout was set to 30 minutes to reflect the amount of time that it may take to complete an online application.

Programme Board is asked decide whether to reduce session timeout to 10 minutes or less or to retain the current period.

8 Secure page browser cache

SES-903 reflects that secure pages within the Portal application can be cached in a user's browser which may allow an attacker to recover information on a shared computer. This has been mitigated by applying a server configuration change to prevent this.

Programme Board is asked to acknowledge this risk has been mitigated.

9 Web servers advertise software type and version

WEB-140 reports that the application web servers advertise Web servers leak ASP.NET version information

This may allow an attacker to target the application based on the server type. This has been mitigated by applying a server configuration change to prevent this.

Programme Board is asked to acknowledge this risk has been mitigated.

10 Web servers leak ASP.NET version information

WEB-165 advises that the application web servers advertise ASP.NET version information. Similarly, to 9 above, this information could potentially be used by an attacker to determine explicit exploits to be attempted. This has been mitigated by applying a server configuration change to prevent this.

Programme Board is asked to acknowledge this risk has been mitigated.