Audit and Governance Committee

Strategic delivery:	☐ Setting standards	☐ Increasing and informing choice	☒ Demonstrating efficiency economy and value

Details:	
Meeting	Audit & Governance Committee
Agenda item	5
Paper number	AGC (04/12/2018) 635
Meeting date	4 December 2018
Author	Jeremy Nolan

Output:	
For information	To provide an update to the Audit and Governance Committee an update on the 2018/19 Internal Audit Plan.
Progress Update	**Progress on 18/19 Audit Plan** **Cyber Security –** The final report for this review has been issued, with a moderate assurance rating given. The report is attached as an annex. **Business Continuity Planning** – The fieldwork for this review is in the early stages. Key information to support the testing has been requested, but at the time of drafting this update, this has still not been received. We have therefore not been able to make any progress on this audit. **GDPR Review** – A start up meeting will be held in early December to discuss the scope of this review, as it is being delivered jointly with the HTA GDPR audit. **Recommendations Follow Up** – Internal Audit have been working closely with HFEA to resolve all outstanding recommendations from previous audit reviews. Progress has been made and we continue to have regular communications to ensure appropriate action has been taken to implement all recommendations.
Actions from previous meeting	None
Organisational risk	☐ Low ☒ Medium ☐ High
Annexes	Annex A – Cyber Security Review

Government Internal Audit Agency

Item 5 AGC (04/12/2018) 635 annex A

Human Fertilisation & Embryology Authority (HFEA)

Review of Cyber Security

Final internal audit report

Date of issue:	28 November 2018
Audit reference:	1819-HFEA-003

Contents

Background and Introduction

The Human Fertilisation and Embryology is the regulator of fertility treatment and human embryo research in the UK. Its statutory functions and regulatory role are set out in the Human Fertilisation and Embryology Act 1990 and the Human Fertilisation and Embryology Act 2008. Their role includes setting standards for clinics, licensing them and providing a range of information for the public, particularly people seeking treatment, donor-conceived people and donors. It is based in London, employs 67 personnel (as at 1st April 2018) and hold the longest register of fertility treatment data in the world, collecting data and statistics for approximately 70,000 fertility treatments each year in the UK from 1991 to present. HFEA hold around 1.25 million records containing personal identifiable information and sensitive medical information. Patient information is input by approximately 80 clinics across the UK via a web portal. The server is held in London in an old estate and is currently in the process of migrating to a cloud-based hosting environment - using Microsoft Azure - due to complete in summer 2019.

The HFEA's vision is "high quality care for everyone affected by fertility treatment" and to realise this their 2017-2020 Strategy is focused on three areas: Safe, ethical, effective treatment; Consistent outcomes and support; and Improving standards through intelligence, which are translated in to six strategic objectives. The achievement of these six objectives are in part dependent on the secure access and use of data/information and technology, for example, use of the website and other channels to increase patients' understanding of the science and evidence base behind treatments, improving the overall quality of treatment, by encouraging world class data and embryo research and clinical trials (not an exhaustive list)[1].

Cyber security refers to the protection of information systems (hardware, software, and associated infrastructure), the data on them and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system or accidentally failing to follow security procedures. The 2015 National Security Strategy confirmed that cyber remains a Tier 1 threat to the UK's economic and national security and it is recognised that cyber-attacks are becoming more frequent and of greater sophistication. At the same time, there has been a significant increase in the services that will be provided digitally, reducing the process burden on users, speeding up delivery and improving the flow of information to enable better quality services.

[1] https://www.hfea.gov.uk/media/2585/business-plan-2018-2019.pdf

As part of the 2018-19 audit plan, a review of Cyber Security was commissioned. This review provides a high-level view over the framework of governance, risk management and control relating to Cyber Security at the HFEA.

Executive summary

Opinion	
Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.	Moderate

Overall, our audit of cyber security has identified a number of areas of good practice in cyber security management, as well as some areas where improvements could be made, as outlined in this summary and presented in detail in the report.

The HFEA's Audit & Governance Committee (AGC) has a specific responsibility to provide oversight of cyber risk management. There is an effective governance structure in place to facilitate this and roles, responsibilities and accountabilities are clearly defined and understood. Whilst membership of AGC aligns fully with HM Treasury guidelines, HFEA could further enhance senior oversight of cyber risk management by recruiting a non-executive member with a background in technology for the AGC.

The AGC considers cyber risk routinely, at each AGC meeting. Currently, HFEA considers that cyber risk is the only strategic risk where the current risk score (9) is outside the risk tolerance (6). However, it is unclear from the Strategic Risk Register update where the gap in control exists and how this is driving the current risk assessment above the risk tolerance threshold. It does not provide details of the specific actions and timescales being undertaken by Management to close the gap and enable the AGC to provide more effective challenge and scrutiny. Providing such information would help HFEA reach their desired position for cyber risk management.

HFEA holds a significant amount of personal, sensitive information (in excess c. 1 million records). This is currently stored on an aging technology estate shared with the National Institute of Clinical Excellence. HFEA are already migrating to a cloud based hosting solution (Microsoft Azure) which aligns with the Cabinet Office's ICT Strategy 'cloud first' principle which is due to complete in the summer of 2019. This will improve the security and resilience of the hosting arrangements.

HFEA are using a data encryption solution for information held on its servers and end point devices (laptops etc.) that aligns with NCSC's guidance to protect information assets classified as up to Top Secret. Therefore, in the event of a data breach, any data accessed should be unreadable providing a robust cyber defence significantly reducing the risk of a successful data breach.

Whilst encryption goes a long way to ensure sensitive information is held securely, it does not help HFEA to prevent its website or web portal from being attacked, disrupting how HFEA prefers to deliver its services to the public and clinicians. In the event of a successful 'denial of service' attack, clinics would be unable to submit applications for treatment and HFEA would have to adopt alternative ways of working to discharge their licensing responsibilities. Failure to do so could result in treatment being delayed or funding windows missed, causing significant reputational damage to HFEA. We have no evidence of a successful denial of service attack, however, HFEA should

explore whether implementing denial of service prevention services such as Akamai as an interim tactical mitigation measure until migration to Microsoft Azure is fully complete is an appropriate option for reducing further cyber risk exposure.

The encryption of sensitive data, and the plans to migrate to new, more secure and resilient hosting arrangements leads us to conclude that a **MODERATE** assurance opinion to be appropriate. We have made 3 Medium and 4 Low priority recommendations to support Management in further enhancing their cyber security control framework.

	High	Medium	Low
Recommendations	0	3	4

Summary of findings

1	**Risk: The absence of a defined information security management framework and governance approach, supported by an appropriate high-level risk assessment could lead to the inconsistent treatment of cyber-security and potential security compromises that could have been avoided.** Mitigation: HFEA has a defined information security management framework and appropriate structures to support the oversight of cyber risk. Scrutiny and challenge could be improved further by appointing to the AGC a non-executive member with a background in technology and upwardly report specific mitigating actions and timescales to bring cyber risk within tolerance to both AGC and the Authority.
2	**Risk: User Awareness and Education - lack of user security policies or user training in recognised good security practices potentially leaving the organisation vulnerable to internal and external threats.** Mitigation: HFEA has appropriate security policies in place and management and staff understand their responsibilities for safeguarding the organisation's information and information assets. Good practices have been established, for example, mandatory information security training. Examination of a selection of policies and interviews with management established that HFEA has introduced and continues to develop a community that fully understands their responsibilities regarding protecting the organisation's information and information assets.
3	**Risk: Ongoing use of ports, protocols and services on networked devices are not managed, increasing the windows of vulnerability available to attackers.** Mitigation: HFEA has reduced the risk of an effective data breach through the use data encryption using an approved NCSC standard. HFEA remains at risk of a denial of service attack and would benefit from investigating whether introducing denial of service attack prevention services such as Akamai, as a mitigating control ahead of migration to Microsoft Azure, would help reduce this risk exposure. The Microsoft Azure hosting design has been independently approved, however, HFEA may benefit from an independent review of the design implementation to confirm that the approved design has actually been deployed.
4	**Risk: The absence of an established security configuration of laptops, servers and workstations using a rigorous configuration management and change controls process increase the risk of unauthorised changes**

	to systems, exploitation of unpatched vulnerabilities and insecure system configurations and increases the number of security incidents. Mitigation: NCSC guidance recommends that organisations should have and maintain baselined security configuration standards for all their operating systems and applications, with any deviation from the standard being subject to change control. These do not currently exist so, to align with NCSC good practice, security configuration standards need to be formally documented. We reviewed the information asset inventory, which details the hardware in place but not software. Without visibility over the software on their devices, including version and patching status, there is a risk of unauthorised software on devices that can be exploited by threat actors. The development of a software and hardware inventory and integrating this with the protective monitoring capability will help support discovery of unauthorised or unpatched software to mitigate the risk of staff unwittingly or consciously introducing cyber vulnerabilities by downloading unauthorised software or connecting unauthorised hardware to the HFEA network. This may cause a disruption to IT systems and services affecting HFEA productivity, but the risk of a successful data loss is significantly reduced as the data is encrypted.
5	**Risk: Failure to implement an incident management capability that can detect, manage and analyse security incidents could compound the impact of a major disruption, fail to address the root cause of incidents and fail to comply with legal or regulatory reporting requirements.** Mitigation: HFEA has an Information Security Incident Management policy in place which provides a framework for reporting and managing incidents, which is underpinned by Business Continuity and Disaster Recovery plans, all of which are tested regularly. This aligns with NCSC good practice guidance. This is further evidence by HFEA's successful recovery from a significant hardware failure which affected a range of core business systems. No loss of data was declared.
6	**Risk: The life-cycle of system and application accounts is not actively managed, including their creation, use, dormancy and deletion, potentially increasing the number of deliberate and accidental attacks.** Mitigation: Policy and standards for user identification and access control have been established and are detailed in HFEA's Access Policy which we consider to be an effective directive control. This, together with HFEA's Role Based Access Controls support good risk management in this context. However, there is less visibility over assurances around third party supplier elevated (privileged) user compliance with the HFEA Access Policy. HFEA should seek periodic assurance that third party elevated user access aligns with the Access Policy, is authorised and appropriate.

Detailed findings 1

Risk 1: The absence of a defined information security management framework and governance approach, supported by an appropriate high-level risk assessment could lead to the inconsistent treatment of cyber-security and potential security compromises that could have been avoided.	**Opinion on risk 1:** Moderate **Risk categories:** Governance for Cyber Security

Findings

Governance

The HFEA governance structure is made up of the Authority, which is the HFEA board and main governance forum. This consists of 12 non-executive members appointed to bring an objective point of view to the board and participate in its eight committees, such as the Audit and Governance Committee (AGC), Statutory Approval Committee and the Executive Licensing Panel.

AGC membership consists of 4 non-executive members, who meet quarterly and are responsible for overseeing corporate governance, risk and audit arrangements and financial matters. None of the current AGC members have a background in technology. They have a specific responsibility for oversight of the cyber security risk therefore to improve challenge and scrutiny of cyber security risk, HFEA may benefit from bringing in a non-executive member with a specific background in technology. AGC Meeting Minutes of October 2018 included updates on General Data Protection Regulation, progress on the Digital Programme and Cyber Security, demonstrating that these are under regular consideration by the AGC.

Overall, HFEA has appropriate governance structures in place to adequately manage cyber security risks, but would benefit from enhanced scrutiny by appointing to the AGC a non-executive member with a background in technology.

Risk management

HFEA has a comprehensive risk management policy and associated processes in place to enable them to effectively identify, monitor and manage risk across the organisation. There is a strategic Cyber Risk recognised by HFEA *"There is a risk that the HFEA has unsuspected system vulnerabilities that could be exploited, jeopardising sensitive information and involving significant cost to resolve".* The residual risk is currently assessed as Medium and HFEA recognises 8 potential vulnerabilities or control weaknesses which could cause the cyber risk to materialise:

- Insufficient governance or board oversight of cyber security risks (relating to awareness of exposure, capability and resource, independent review and testing, incident preparedness, external linkages to learn from others).

- Changes to the digital estate open up potential attack surfaces or new vulnerabilities. Our relationship with clinics is more digital, and patient identifying information or clinic data could therefore be exposed to attack.
- There is a risk that IT demand could outstrip supply and so IT support doesn't meet the business requirements of the organisation and so we cannot identify or resolve problems in a timely fashion.
- Confidentiality breach of Register or other sensitive data by HFEA staff.
- There is a risk that technical or system weaknesses lead to loss of, or inability to access, sensitive data, including the Register.
- Business continuity issue (whether caused by cyberattack, internal malicious damage to infrastructure or an event affecting access to Spring Gardens).
- The corporate records management system (TRIM) is unsupported and unstable and we are carrying an increased risk of it failing. The organisation may be at risk of poor records management until the new system is functioning and records successfully transferred.
- Cloud-related risks.

On reviewing the Strategic Risk Register update presented to the October 2018, AGC identified the risk of staff causing a cyber-attack, either accidently or deliberately, which was a contributing factor to the strategic-level cyber risk being deemed outside tolerance (target risk score 6; actual risk score 9). Although this demonstrates active senior level engagement in managing cyber risk, the Strategic Risk Register update does not clearly articulate where controls are currently below those expected for the individual cyber risk elements (see bulleted list above) and the specific steps to be taken to bring risk exposure within tolerance. We recommend that the specific mitigating actions for individual risk elements, including timelines, to bring cyber risk exposure within tolerance are reported to the next AGC and Authority meetings.

Implications and recommendations

HFEA has a defined information security management framework and appropriate structures to support the oversight of the cyber risk. Scrutiny and challenge could be improved further by appointing to the AGC a non-executive member with a background in technology. The management of the cyber security risk should be improved so there is a clear articulation of the controls 'gap' for each element of the cyber risk and necessary steps required to reduce the risk exposure (current score 9) to the desired level (residual risk score 6).

Recommendations

Management should consider appointing a non-executive member to the Audit & Governance Committee who has a background in technology.

Management should ensure that the Strategic Risk Register update is improved to clearly articulate details of individual cyber risk element control gaps, the necessary specific mitigating actions, including timelines, to bring cyber risk exposure within tolerance and report these to the next AGC and Authority meetings.

Detailed findings 2

Risk 2: User Awareness and Education - HFEA do not have user security policies or train their users in recognised good security practices potentially leaving the organisation vulnerable to internal and external threats.	**Opinion on risk 2:** Substantial **Risk categories:** User Awareness and Education

Findings

HFEA has an Information Governance Policy in place which describes their approach to information governance and information handling, associated roles and responsibilities, for example, SIRO, management and staff. This overarching policy is complemented by a comprehensive range of policies and procedures that provide guidance and support to management and staff. Examination of a selection of policies and interviews with stakeholders established that management and staff have a clear understanding of their responsibilities for safeguarding the organisation's information, information assets and of cyber security risks. There is a learning and development policy in place to ensure management and staff received the appropriate training, for example:

- All personnel undertake annual mandatory Information Security training, which is monitored for completion;
- Changes to policies and procedures are communicated to everyone in All Staff Bulletins;
- To address GDPR requirements, policies were reviewed and revised and the organisation has built in periodic reviews;
- Personal responsibility for complying with corporate security policies (and the consequences of abuse) are re-enforced during induction and changes of duty;
- Access management and new user process sets out responsibilities for using HFEA equipment and information and staff acknowledge that they understand their responsibilities as part of their log-in process; and
- A recent security incident resulted in all staff being reminded about good practice when travelling with HFEA devices.

As a result of the migration to Microsoft Azure, HFEA is in the process of reviewing and updating their existing information security management policies and procedures to ensure these align with the ISO 27001:2013 Information Security Management Standard framework of policies and procedures. Whilst we consider the existing policies to be appropriate, this is a good opportunity to ensure the policies adequately reflect the changing landscape of moving to a cloud solution.

Implications and recommendations

HFEA has appropriate policies and processes in place to ensure staff and management are fully aware of their information security responsibilities to help safeguard the organisations information. No recommendations have been made.

Detailed findings 3

Risk 3: Ongoing use of ports, protocols and services on networked devices are not managed, increasing the windows of vulnerability available to attackers.	**Opinion on risk 1:** Moderate **Risk categories:** Network Security

Findings

HFEA holds over c.1 million patient records containing sensitive personal and medical information. HFEA hosts its aging legacy technology estate in an office location shared with the National Institute for Clinical Excellence (NICE). Aging technology estates increase cyber risk security exposure, for example, software and hardware can be out of vendor support meaning that should new malware be created, a security patch will not be developed to protect against the new vulnerability. The data held by HFEA on its servers and desktops/laptops is encrypted using the AES-256 encryption standard which the National Cyber Security Centre (NCSC) has approved to protect information classified up to Top Secret. This provides an effective mitigation against a data breach exploiting any vulnerabilities associated with ports, protocols or services on network devices as any data obtained should be unreadable. However, this does not protect HFEA from a denial of service attack or similar which would prevent the public, fertility clinics and researchers from accessing the HFEA website and web portal.

HFEA recognises the need to upgrade its technology estate. However, as a small organisation, it needs a cost-effective way of acquiring, running and maintaining new hardware and software. In line with the Cabinet Office's ICT Strategy of 'Cloud First', HFEA has commenced a programme of activity to migrate systems and data to the 'cloud' with Microsoft Azure providing hosting services which is expected to complete by the summer of 2019. This should reduce IT running and investment costs for HFEA as the cost of hosting services is cheaper for Cloud providers than small organisations. Cloud hosting, if appropriately designed and implemented, should also provide improved security and resilience controls. The latter is particularly important to reduce the risk of a denial of service attack or similar on HFEA's website and web portal.

In the meantime, HFEA are dependent on NICE's protective monitoring capability to detect unusual patterns of activity such as unexpected surges in the number of access attempts to the website which could indicate a potential denial of service attack. We found no evidence that a denial of service attack has taken place to date, but such an attack could have a significant impact on HFEA. For example, if the web portal is unavailable for an extended period, say 1 week, this could delay a clinic's ability to submit an application for approval by HFEA. It is unclear how quickly the web portal could be restored. HFEA would benefit from investigating whether further mitigations such as the use of a denial of service attack prevention service – Akamai, for example - should be put in place to reduce this risk.

HFEA cloud hosting design for Microsoft Azure was undertaken by a specialist IT design company (Alscient) and has been assured by a CLAS consultant. This provides assurance that the design meets NCSC's Cloud Security Guidance requirements. HFEA would benefit from

an independent review of the hosting design implemented by Microsoft Azure to provide assurance that the required design has actually been implemented.

Implications and recommendations

HFEA has reduced the risk of an effective data breach through the use data encryption using an approved NCSC standard. HFEA remains at risk of a denial of service attack and would benefit from investigating whether introducing denial of service attack prevention services as a mitigating control ahead of migration to Microsoft Azure would help reduce this risk exposure. The Microsoft Azure hosting design has been independently approved. HFEA would benefit from an independent review of the design implementation to confirm that the approved design has actually been deployed.

Recommendations

Management should consider introducing denial of service prevention services such as Akamai as a tactical mitigation ahead of the completion of migration to Microsoft Azure expected in the summer of 2019.

Management should commission an independent review of the approved Microsoft Azure hosting design deployment to provide assurance that the design approved has been deployed.

Detailed findings 4

Risk 4: The absence of an established security configuration of laptops, servers and workstations using a rigorous configuration management and change controls process increase the risk of unauthorised changes to systems, exploitation of unpatched vulnerabilities and insecure system configurations and increases the number of security incidents	**Opinion on risk 1:** Moderate **Risk categories:** Secure configuration

Findings

NCSC guidelines recommend that organisations should have and maintain baselined security configuration standards for all their operating systems and applications, with any deviation from the standard being subject to change control. These configurations should be formally documented and maintained as software is updated or patched, new security vulnerabilities are reported, and configurations are modified to allow the installation of new software or support new operational requirement. We understand that these are not in place for HFEA; instead the IT Service Management Team provision, build and configure end-point devices to ensure the user has the appropriate access and applications required for their role and approved by management. To align with NCSC's guidelines, we recommend that management formally document security configuration standards and develop a process to maintain these on an ongoing basis.

We reviewed the information asset inventory and confirmed that it details the end-point devices in use but not software. Without an approved list of software, including version and patching status, the effectiveness of any protective monitoring regime is diminished; we would expect the information on the asset inventory to inform a 'whitelist' of approved devices and software which would then be monitored against with security alerts being raised when unauthorised devices connect to the network or staff attempt to download unauthorised software. There remains a risk that unauthorised software exists on devices that can be exploited by threat actors. Such an attack could disrupt HFEA's day-to-day activity through a loss of IT systems and services. However, the risk of a successful data breach resulting in a loss of sensitive data is significantly reduced by such data being encrypted and therefore unreadable if inappropriately accessed.

Access to laptop devices (predominantly MS SurfacePro) are securely configured by activating Bitlocker which provides encryption at the Operating System level. This is a standard configuration and we are content this provides an effective control in preventing unauthorised access. In addition, HFEA has deployed Microsoft InTune to manage the deployment of fixes from Microsoft and enforce device policies to reduce the risk of cyber-attacks which, again, we consider to be an effective control.

HFEA are migrating elements of their infrastructure to Microsoft Azure Cloud (Azure) and this is due to complete by summer 2019. This aligns with the cabinet Office's ICT strategy of 'cloud first' hosting principle. Azure Update Management ensures that Windows operating system updates classified as critical or security are automatically applied and patching updates are run every week. We are content that this

helps manage cyber risks for system or services hosted in Azure though we are unsighted on the security and resilience arrangements for the legacy systems therefore we are not able to comment of their control rigour at this time.
Implications and recommendations
Aligning more closely with NCSC guidance will help support more robust cyber risk management as will improving discovery and monitoring capability. This is especially important given the confidential nature of information resident in HFEA systems and their acknowledgement that strategic level cyber risk is considered to be outside tolerance. **Recommendations** Management should formally document baselined security configuration standards and develop a process to maintain these on an ongoing basis. Management should develop a software and hardware inventory and integrate this with the protective monitoring capability to help prevent the downloading of unauthorised software by staff and detect instances of unauthorised hardware connecting to the HFEA networks and unauthorised software put onto the HFEA network by external attackers.

Detailed findings 5

Incident Management – Failure to implement an incident management capability that can detect, manage and analyse security incidents could compound the impact of a major disruption, fail to address the root cause of incidents and fail to comply with legal or regulatory reporting requirements	**Opinion on risk 5:** Substantial **Risk categories:** Incident Management

Findings

HFEA have an Information Security Incident Management policy in place which provides a framework for reporting and managing incidents affecting security of information and IT systems, loss of information and information security concerns. This process aligns with NCSC guidance in terms of *'establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact'*. The policy and underpinning processes re-enforce everyone's role and responsibilities in reporting and managing security incidents and signposts them to where to report incidents and what action to undertake.

All the plans supporting incident management, for example Business Continuity are in place, tested and the subsequent outcomes evaluated and used to inform improvements to the organisation's incident management plan. Outcomes from real-time incidents and tests are reported to the AGC.

Our examination of the policy and processes, the supporting plans and the AGC board papers confirmed that the processes are in place, being tested and have been successfully applied in response to an actual incident. Further evidence of this lies in HFEA's response to a system outage resulting from a server failure in April 2018. This was deemed to be a significant incident though the majority of systems were restored rapidly; no data losses were declared.

Implications and recommendations

HFEA have established policies and procedures to manage incidents well have done so in a real-world scenario. We are content that the evidence we have examined affirms that incident management is well governed and controlled. No recommendations have been made.

Detailed findings 6

Managing User Privileges – the life-cycle of system and application accounts is not actively managed, including their creation, use, dormancy and deletion, potentially increasing the number of deliberate and accidental attacks.	**Opinion on risk 6:** Moderate **Risk categories:** Managing User Privileges

Findings

Policy and standards for user identification and access control have been established and are detailed in the organisation's Access Policy. The policy is available to all staff, amendments are emailed to everyone as a 'push' communication to ensure all staff are signposted to any changes and the policy is complemented by several other policies and processes relating to managing user access. We consider the suite of policies and associated procedures and guidance provide all users with the necessary support to access and use HFEA information systems.

Role Based Access Controls (RBAC) are used to limit user privileges (rights and permissions) to systems, services, information and resources needed to fulfil their role. The number of elevated (privileged) user accounts is limited to the IT Service Management team, who are responsible for allocating user permissions once authorised by management. All data in the servers and the end point devices is encrypted reducing the risk of successfully obtaining unauthorised access to sensitive records.

Discussions with management and examination of the organisation's security policies confirmed that processes and procedures are in place to manage and review user accounts from creation through to deletion when the user leaves. We have not discovered any evidence of any weakness in these processes. However, it is not visible how HFEA obtain assurances from 3rd party suppliers (Azure and Alscient) that their staff comply fully with the HFEA Access Policy.

Implications and recommendations

HFEA has the appropriate directive controls in the form of a comprehensive suite of policies to describe the process and limitations in staff being granted access to systems and services and the associated Role-Based Access Controls. However, we are unclear as to how this is managed in the supply chain.

Recommendation

Management should consider seeking periodic assurances from Azure and Alscient over the management of elevated users, the number with access to HFEA infrastructure, confirmation that the privilege account actions are appropriate and that they cannot see HFEA data or access the systems.

Annex 1: Management action plan

Risk 1:	**The absence of a defined information security management framework and governance approach, supported by an appropriate high-level risk assessment could lead to the inconsistent treatment of cyber-security and potential security compromises that could have been avoided.**				
Opinion on Risk 1:	Moderate				
Recommendation(s)		**Priority**	**Action agreed**	**Target date**	**Owner**
1.1	Management should consider appointing a non-executive member to the Audit & Governance Committee who has a background in technology.	Medium	To be considered by AGC	March 2019	TBC
1.2	Management should update the Strategic Risk register to include details of individual cyber risk element control gaps, the necessary mitigating actions, including timelines, to bring cyber risk exposure within tolerance and report these to the next AGC and Authority meetings.	Medium	We have undertaken further cyber security (penetration) testing of the new digital systems such as PRISM and the Register, to ensure that these remain secure. The results have not revealed any significant issues. SMT raised the tolerance level of this risk to 9 in November, reflecting that though we believe our cyber controls are fit for purpose, the context in which we operate, with a high level of national cyber risk, means we are tolerating a higher level of risk. There has been no evidence to suggest the national cyber risk has been further heightened. We	No action to be taken	Not applicable

			continue to assess and review the risk and take action as necessary to ensure our security controls are robust and are working effectively. This strategic risk register has been updated to reflect the above and it will continue to be regularly reviewed as part of our risk monitoring cycle.		

Risk 3:		**Ongoing use of ports, protocols and services on networked devices are not managed, increasing the windows of vulnerability available to attackers.**			
Opinion on Risk 3:		Moderate			
Recommendation(s)		**Priority**	**Action agreed**	**Target date**	**Owner**
3.1	Management should consider introducing denial of service prevention services such as Akamai as a tactical mitigation ahead of the completion of migration to Microsoft Azure expected in the summer of 2019.	Medium	This has been carefully considered. Given a) the procurement and implementation timeline of a specialist DDoS system, and b) we have considered the risk of unavailability of data. On that basis of the risk assessment we have agreed to accept this risk and we will review again in summer 2019.	No action to be taken	Not applicable
3.2	Management should commission an independent review of the approved Microsoft Azure hosting design deployment to provide assurance that the design approved has been deployed.	Low	The configuration has been specified by industry leading experts (Alscient) and assurance on the configuration has been sought from a CLAS consultant. The third and final penetration test by third party NTA will review the security configuration to identify any potential weaknesses.	No action to be taken	Not applicable

			Given it assesses the effectiveness of the security controls specified as part of the agreed design, it will provide assurance that the design approved has been deployed and that the controls are effective.		

Risk 4:		**The absence of an established security configuration of laptops, servers and workstations using a rigorous configuration management and change controls process increase the risk of unauthorised changes to systems, exploitation of unpatched vulnerabilities and insecure system configurations and increases the number of security incidents.**			
Opinion on Risk 4:		Moderate			
Recommendation(s)		**Priority**	**Action agreed**	**Target date**	**Owner**
4.1	Management should formally document baselined security configuration standards and develop a process to maintain these on an ongoing basis.	Low	Agreed – these will be documented and reviewed on a quarterly basis	01 March 2019	Dan Howard, Chief Information Officer
4.2	Management should develop a software and hardware inventory and integrate this with the protective monitoring capability to help support discovery of unauthorised or unpatched software to mitigate the risk of staff unwittingly or consciously introducing cyber vulnerabilities and/or to reduce the risk of unauthorised hardware connecting to the HFEA networks.	Low	We will create a software inventory of approved software and annually review the results of the software audit to ensure only authorised software is present on the network. No user has administrative permissions by default on HFEA devices which in turn prevents users installing unauthorised software. We use Microsoft Insight to ensure	01 January 2019	Dan Howard, Chief Information Officer

			essential security patches are applied as required.		

Risk 6:		**Managing User Privileges – the life-cycle of system and application accounts is not actively managed, including their creation, use, dormancy and deletion, potentially increasing the number of deliberate and accidental attacks.**			
Opinion on Risk 6:		Moderate			
Recommendation(s)		**Priority**	**Action agreed**	**Target date**	**Owner**
6.1	Management should consider seeking periodic assurances from Azure and Alscient over the management of elevated users, the number with access to HFEA infrastructure, confirmation that the privilege account actions are appropriate and that they cannot see HFEA data or access the systems.	Low	Agreed – this will happen on a quarterly basis	First review March 2019	Dan Howard, Chief Information Officer

Annex 2: Objectives, scope and limitations

Objectives:

This review will provide an independent and objective assurance on the framework of governance, risk management and control relating to Cyber Security.

Scope and Limitations:

This review will provide a high-level view over the governance, policies, processes, standards, procedures, management information and other control activities introduced to reduce the risks associated with Cyber Security and will examine:

- Governance for cyber security:
  - Understanding of the risks and the determination of an appropriate risk appetite;
  - Roles, responsibilities and accountabilities of the individuals responsible for cyber security; and
  - The development, implementation and maintenance of the strategy, policies and procedures, for example information security management framework, risk management policy, procedures and risk appetite statement.
- Secure Configuration:
  - Examine baselined security configurations for laptops, servers and workstations and the associated configuration management and change controls process; and
  - Software patching regime.
- Network Security:
  - Intrusion detection systems, monitoring and response.
- Malware prevention:
  - Updating of malware prevention software.
- Removable Media:
  - Review of policies on use of removable media and enforcement of those policies.
- Mobile and Home Working:
  - Review of scope of risk assessments and policies for mobile options; and
  - Protection of data-at-rest and of data-in-transit.

This review will **not** examine:

- The effectiveness of cyber security risk management and response within LGSCO; and
- Compliance with the General Data Protection Regulation.

We will undertake this review subject to the limitations outlined below:

Internal Audit
Internal controls systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgement in decision-making, human error, control processes being deliberatively circumvented by employees and others, management overriding controls and the occurrence of unforeseeable events.

Future periods
Our assessment of controls is for the period specified only. Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in the operating environment, law, regulation or other changers; or
- The degree of compliance with policies and procedures may deteriorate.

Distribution:

Richard Sydee
Dan Howard
Nick Jones
Steve Morris

Cameron Robson
Jeremy Nolan
Tony Stanley

Author:

Alistair Burgess

Annex 3: Our classification systems

Opinion

Substantial	The framework of governance, risk management and control is adequate and effective.
Moderate	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
Unsatisfactory	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

Recommendations

Priority	Definition	Action required
High	Significant weakness in governance, risk management and control that if unresolved exposes the organisation to an unacceptable level of residual risk.	Remedial action must be taken urgently and within an agreed timescale.
Medium	Weakness in governance, risk management and control that if unresolved exposes the organisation to a high level of residual risk.	Remedial action should be taken at the earliest opportunity and within an agreed timescale.
Low	Scope for improvement in governance, risk management and control.	Remedial action should be prioritised and undertaken within an agreed timescale.