Implementation of Audit Recommendations – Progress Report

Strategic delivery:	☐ Setting standards	☐ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item	4e		
Paper number	[AGC (21/03/2017) 529 WEC]		
Meeting date	21 March 2017		
Author	Wilhelmina Crown - Finance & Accounting Manager		
Output:			
For information or decision?	Decision		
Recommendation	AGC is requested to review the enclosed progress updates and to comment as appropriate.		
Resource implications	As noted in the enclosed summary of outstanding audit recommendations		
Implementation date	As noted in the enclosed summary of outstanding audit recommendations		
Organisational risk	☐ Low	☐ Medium	☐ High

Report

1.1. This report presents an update to the paper presented to this committee at its meeting in December 2016.

1.2. The recommendations agreed as completed by this committee in December have been removed.

1.3. The recommendations and follow up actions from the latest audit reports (Board Effectiveness Assessment, Information Standards and Cloud Cyber Risk Assessment - advisory) which will be presented to this meeting have been included.

1.4. Recommendations are classified as high (red), medium (amber) or low (green).

1.5. Seven new recommendations were received with two noted as medium and five as low.

1.6. Recent updates received from Action Managers are recorded under a February 2017 heading in this document.

1.7. Three recommendations (including the new items) are noted as completed with rest due to be completed by end May 2017.

Recommendation

AGC is requested to review the enclosed summary of recommendations and updated management responses and to advise whether they have any comments or queries in respect of them.

Annex 1: Summary of Recommendations

Recommendation Source	Status / Actions	2016/17	Total
Internal – *DH Internal Audit*	*Complete*	*3*	***3***
	To complete	*5*	***5***
COUNT		***8***	***8***

FINDING/*RISK*	Recommendation	Agreed actions / Progress Made	Owner/Completion date
2016/17 – INTERNAL AUDIT CYCLE			
INCOME GENERATION			
1.	**Follow-up procedures with those clinics that do not submit activity data could be more robust.**		
Clinics that have not submitted data to the HFEA for a period longer than one month are identified by the Head of Information and the Senior Network Analyst on a monthly basis. However, this is primarily to allow accurate accruals and deferrals of income to be made rather than to enable HFEA to identify clinics that may be having issues in submitting data. Some follow up is performed if a particular issue is noted, but this is on an ad hoc basis and there is no formalised process to follow-up all clinics to identify whether data should have been received.	The monthly report of clinics which have not submitted data for one month should be used as a basis to ensure that clinics have been, or are, contacted or otherwise checked to identify the reasons and any action that HFEA may need to take to resolve any issues. The reasons for any problems that clinics are experiencing should be documented and progress monitored. The record could be cross referenced to the IT support system ticket number(s) where the cause is an IT matter	Using the monthly report of clinics which have not submitted data for a month, a document will be created listing the clinics and the problems they are experiencing, the person responsible for resolving the issue and the status of the problem. This will be discussed in a monthly meeting with actions designated to appropriate individuals to resolve them and to contact the clinic as necessary. **November 2016 update** Check has already been done for November. The appropriate Register SOP will be updated prior to December's, to enable monthly checking. **February 2017 update** This process has not yet been formally adopted and a documentation of the process has not yet been complete. However, monthly checks are performed by the HOI. It is anticipated that both will now be completed by end February 2017 The SOP is updated and was approved by the Director of Compliance **Recommendation complete**	***Head of Information*** **Date**: September 2016 billing run **End December 16** **End February 2017** **COMPLETE**

FINDING/*RISK*	Recommendation	Agreed actions / Progress Made	Owner/Completion date
BOARD EFFECTIVENESS SELF-ASSESSMENT			
2. Ensure that board members are briefed or receive alerts on key developments			
Interviews with the board members identified that some members felt that there were some gaps in the sharing of information between the board meetings, especially for those board members who are not involved in the work of the Authority's committees. In particular, the board members noted that where the Authority is involved in legal cases, the members would welcome receiving updates before the cases become public knowledge through the media. In addition, while it was reported that the working papers provided for the board include the right level of detail and also an update on previously agreed actions, a few comments were received about providing board members with clearer updates on the progress, completion of agreed actions and implementation of policies, especially where the implementation may be over a longer period of time. Without clear and timely updates, board members may not have full visibility of current cases and legal challenges to the Authority's decisions. This may impact on how they respond when matters that have reached the public domain are raised with them. Board members may also lack visibility on the rate of progress and completion of actions and implementation of decisions, which could impact on their ability to hold the Executive team to account for timely progression and implementation.	Ensure that board members are briefed or receive alerts on any key developments, including decisions and legal cases, on a timely basis to help prepare them for any questions that may arise. Ensure that updates on progress and implementation of agreed actions and policies provide a full summary of progress made, next steps and, where relevant, an indication of whether progress is in line with the original timetable and if the originally intended completion date should be achieved.	We recognise that the part time nature of Board members' role does not always allow them to keep up to date with key developments. We currently do a number of things to address this - weekly press updates, private legal updates, regular briefing meetings between Chair, Deputy Chair, Chair AGC and Chief Executive – but accept that we may need to do more. We will ask members what additional information they would find most useful. **We will consider how the strategic performance report might encompass an action log (or similar) to capture progress over time.**	***Chief Executive*** **30th May 2017**
3. Consider developing additional training and support for new board members			
Positive feedback was received in respect of the legal training provided as part of the induction for new board members. However, some further induction training on corporate governance and the board's operational framework would be welcomed. Some members would welcome more training and development support around the role of the board members and specifically their responsibilities and work expectations outside of meetings. Further discussion with the Chair and the Chief Executive confirmed that conversations about the role, responsibilities and work expectations are held informally with the new board members. However, formalisation of those discussions in a more structured training approach may assist clarity about the board members' role, and could include more clarification of the expectations between board meetings.	Consider developing additional training and support for new board members around the operation of the board, corporate governance and providing additional guidance on being an effective board member, including activities between board meetings.	Chair and Chief Executive currently provide informal induction and support for new members, alongside formal legal training. We will discuss with members what more formal corporate induction would be most helpful	***Chief Executive*** **30th May 2017**

New board members may lack clarity on how the board operates, its decision making processes and what is expected of board members, particularly between meetings. If this was to be the case, board and individual effectiveness could be impaired, and this may be particularly relevant at times of change in board membership.			
INFORMATION STANDARDS			
4.	**The workflows within the CMS system are not currently configured to require approvals or enforce segregation of duties between writing, uploading and releasing publications to the new website.**		
The CMS system is used to manage publication of documents on to the new HFEA website. CMS workflows can be configured to require approval from designated individuals and ensure that different users are involved at the uploading and releasing stages. However during our testing we found that this functionality is not currently in place for the new website and that this has resulted in two sets of exceptions identified below. Management confirmed that this was because issues had been experienced with CMS, including approvers not being notified when publications are released. These issues are currently with the CMS team for resolution and management has confirmed that appropriate workflows will be in place by 6th March 2017. During our testing, we identified three publications which were published prior to receiving approval: 1) Our committees and panels 2) Our partners; and 3) Meet our Authority members/our board. The following two publications were uploaded and published by the same individual; 1) Applying to use our data for research; and 2) Making a complaint about a fertility clinic. *As the public has access to the new website there is a risk that inaccurate or inappropriate information could be published which could undermine HFEA's stated objective of building trust in their regulation of human tissue. Furthermore if the publications were of poor quality this might lead to confusion amongst users which may lead to higher levels of individual requests for help and/or guidance. This may have an impact on use of resources and value for money*.	• Until the issues within CMS are resolved, approval should be obtained for all publications prior to release onto the website. • Ensure that the workflows within CMS are appropriately designed to provide segregation of duties between upload and release and that these are implemented as soon as possible.	We acknowledge this and agree with the recommendation. ***We have addressed this by making sure that either the Head of Engagement or the Director of Strategy approves new content before it is published through the CMS*** ***We will turn on the CMS workflow functionality on 1 March*** **Recommendation complete**	***Head of Engagement*** 1 March 2017

5.	**Per HFEA guidance, an evidence source, i.e. a staff member with appropriate knowledge and expertise, is not required to formally approve the draft publication**			
The 'Producing corporate website content' guidance document, requires that the communications team works with an evidence source to gain the facts that they need to update or create content and decide on timelines for the information to be produced. The evidence source is usually a member of staff with the relevant knowledge and expertise. However, it is not required that the evidence source formally approves the publication to verify the factual accuracy prior to release. From our testing we noted that for six out of the eight publications tested, there was written approval from the evidence source, which indicates that this is occurring in practice in some cases, but we also noted two documents where formal approval was not obtained. The two publications for which we were unable to obtain evidence of written approval from the evidence source were 'Our partners' and 'Applying to use our data for research'. Management confirmed that verbal approval was provided for the 'Our partners' page and for 'Applying to use our data for research', we did see evidence of working with the evidence source, although not final approval. As the corporate information contained on the website can vary in the risk attached to any inaccuracies, the requirement for review and approval by the evidence source could be applied on a risk based approached, taking into account the type of information being published. *The information provided could be of poor quality and/or inaccurate which could undermine HFEA's stated objective of building trust in their regulation. Furthermore, if the evidence source does not sign off the publication there might be a lack of accountability should the publication prove to be inaccurate.*	Consideration should be given to require evidence sources to provide formal approval of each publication. As the corporate information contained on the website can vary in the risk attached to any inaccuracies, this requirement could be applied on a risk based approached, taking into account the type of information being published. The guidance document should be updated for any changes to policy.	We acknowledge this and agree with the recommendation. ***We will amend the guidance document so that evidence sources must formally approve any changes.***	***Head of Engagement*** 1 April 2017
6.	**Lack of written evidence of approval from the Head of Engagement and/or a Director for six of the eight publications selected for testing.**			
The guidance document requires that corporate publications are subject to appropriate review before release. This includes a final sign off from a Director and/or by the Head of Engagement. During our review we were unable to locate evidence of formal written approval for six publications. In discussion with the Head of Engagement it was stated that verbal approval was provided on each of these occasions and, therefore, this is considered a documentation issue. The publications for which we were unable to review evidence of approval were: 1) Our committees and panels 2) Our partners 3) Making a complaint about a fertility clinic 4) Meet our Authority members/our board 5) Applying to use our data for research 6) Home Page	All approvals should be in writing to evidence that all publications have been appropriately reviewed and approved, and have a complete audit trail.	We acknowledge this and agree with the recommendation. ***We will clarify the guidance and ensure an email is sent to the author to confirm approval***	***Head of Engagement*** 1 April 2017

As the public has access to the new website there is a risk that inaccurate information could be published which could undermine HFEA's stated objective of building trust in their regulation if appropriate review has not been undertaken. In addition, if the publications were of poor quality this might lead to confusion amongst users which may lead to higher levels of individual requests for help and/or guidance, impacting use of resources. If approval is not evidenced, there is greater risk that a publication may be released which has not been appropriately reviewed and approved, which increases these risks.			
CLOUD CYBER RISK ASSESSMENT (ADVISORY			
7. Cloud lock-in			
Cloud lock-in is a situation in which an organisation is unable to migrate their infrastructure to a cloud competitor due to using proprietary technologies that are incompatible with those of competitors. HFEA's current cloud infrastructure has been designed to ensure cloud lock-in does not occur; and	Cloud lock-in - we recommend HFEA to update their Change Management policies to ensure cloud lock-in is considered before any cloud related change occurs such as the introduction of new infrastructure. This will reduce the likelihood of HFEA being locked-in with Microsoft Azure in the future.	Agreed. Cloud lock in will be considered in advance of selection of any PAAS products. **Recommendation complete**	***Head of IT*** ***Complete***
8. Business Continuity (Advisory)			
Using a public cloud service such as Microsoft's Azure Cloud requires a network connection to the outside world (internet). A network related incident at the HFEA office could result in staff being unable to access key services hosted on the Azure Cloud	We recommend HFEA to update their Business Continuity policies to ensure it has appropriate plans and procedures in the event of an incident, such as network failure impacting services hosted on the Azure Cloud. This could be something simple as allowing staff to work from a secure environment such as their home via a secure VPN connection.	Agreed. IT staff can already access Azure services from remote locations. General HFEA staff can access Office 365 from home. ***Remote access in place.*** We will investigate divergent route network connectivity for Spring Gardens. ***Divergent route to be investigated***	***Head of IT*** ***Complete*** ***by end of April 2017***

Health Group Internal Audit

Reference: DHX216008005
DRAFT REPORT
Human Fertilisation and Embryology Authority
March 2017

Health Group Internal Audit provides an objective and independent assurance, analysis and consulting service to the Department of Health and its arms length bodies, bringing a disciplined approach to evaluating and improving the effectiveness of risk management, control and governance processes.

The focuses on business priorities and key risks, delivering its service through three core approaches across all corporate and programme activity:

- **Review and evaluation** of internal controls and processes;
- **Advice to support management** in making improvements in risk management, control and governance; and
- **Analysis of policies, procedures and operations** against good practice.

Our findings and recommendations:

- Form the basis of an independent opinion to the Accounting Officers and Audit Committees of the Department of Health and its arms length bodies on the degree to which risk management, control and governance support the achievement of objectives; and
- Add value to management by providing a basis and catalyst for improving operations.

Report Name:

Cloud Cyber Risk Assessment

Overall report rating: MODERATE

Status: DRAFT

For further information please contact:
Cameron Robson - 01132 54 5515
1N16 Quarry House, Quarry Hill, Leeds, LS2 7UE

CONTENTS **PAGE**

Date fieldwork completed:	10/02/2017
1st draft report issued:	06/03/2017
Management responses received:	xx/xx/2017
Final report issued	xx/xx/2017

Report Author: Asim Khan/ Jayne Goble

Version №: Draft V0.1

Distribution List – Draft Report

Main recipient(s)

David Moysen	Head of IT HFEA
Morounke Akingbola	Head of Finance HFEA
Richard Sydee	Director of Finance and Resources

Cc(s)

Cameron Robson	Group Chief Head of Internal Audit
Karen Finlayson	Head of Internal Audit

Distribution List – Final Report

As above

EXECUTIVE SUMMARY

1. Introduction

1.1 The 'McCracken review' of the HFEA in 2013 recommended that the HFEA modernise its systems and processes to both save on costs and reduce the administrative burden on clinics. The Information for Quality ("IfQ") programme is the HFEA's response to the recommendations, made in the McCraken review. The IfQ programme is designed to transform the HFEA's approach to information both in how staff collect data and how staff publish information.

1.2 The provision of IT services is essential for the delivery of HFEA's IfQ programme as well as HFEA's business. For example, management have recently consolidated HFEA's existing IT infrastructure into a predominantly cloud based environment. Management have selected an Azure service platform to provide HFEA with SQL and NoSQL data services with built-in support (as well as tech support), health monitoring and other services. SQL and NoSQL are Microsoft databases that are capable of handling mission-critical workloads. Microsoft Azure is therefore intended by management to give HFEA the service platform needed to achieve the goals of the IfQ programme.

1.3 An important step when implementing HFEA's Microsoft stack and Azure service platform is to ensure the ongoing provision of these services, as well other HFEA ICT services, are secure to meet HFEA's corporate needs.

1.4 This review has been commissioned as part of the FY16/17 internal audit plan, to identify security risks relating to a cloud environment and identify any gaps in HFEA's security control framework. The review was delivered via a workshop, where industry specialists with management determined the business impact and likelihood of potential risks related to cloud hosting. This outcome of the workshop provided management with a prioritised list of high, medium and low cloud security risks relevant to HFEA's IT environment. Recommendations were provided when there was a requirement to enhance the adequacy and effectiveness of HFEA's controls for their infrastructure hosted in the Cloud (see Appendix B for evidence).

2. Review Conclusion

2.1 The rating for the report is **Moderate** - some improvements are required to enhance the adequacy and effectiveness of the controls for the infrastructure hosted on the Microsoft Azure Cloud. However, no high risks were identified in HFEA hosting their infrastructure on the Microsoft Azure Cloud platform. In addition, although the business risk remains the same for cloud hosted infrastructure, the likelihood of risks occurring are reduced due to the controls Microsoft Azure (cloud provider) have in place.

2.2 HFEA have an appropriate contractual agreement in place that ensures Microsoft are accountable for maintaining a certain level of service. Microsoft Azure adheres to the internationally recognised ISO27001 certification that ensures they have appropriate internal and external security processes, which reduces the likelihood of an intruder accessing the infrastructure physically or remotely. Their Data Centres are highly resilient and are generally located in remote locations that reduce the likelihood of major events such as terror incidents occurring.

In addition, Microsoft Azure adheres to the UK government initiative Government Cloud (G-Cloud). It has been created to ease procurement of cloud services by government departments and promote government-wide adoption of cloud computing. G-Cloud comprises a series of framework agreements that includes data in transit protection, asset protection and resilience, data separation between consumers, external interface protection, and logical and physical security.

Microsoft's Service Trust Portal provides independently audited compliance reports for the Azure Cloud platform as evidence of all their certifications including G-Cloud and ISO27001.

3. Summary of Findings

3.1 The review is intended to help the Head of Engagement enhance the effectiveness and implementation of the standards for cloud environment by providing an independent and objective view of the control in place. Where required, recommendations have been provided to enhance the adequacy and effectiveness of HFEA's controls for their infrastructure hosted in the Cloud.

3.2 The findings from our work are summarised below:

- Cloud lock-in is a situation in which an organisation is unable to migrate their infrastructure to a cloud competitor due to using proprietary technologies that are incompatible with those of competitors. HFEA's current cloud infrastructure has been designed to ensure cloud lock-in does not occur; and
- Using a public cloud service such as Microsoft's Azure Cloud requires a network connection to the outside world (internet). A network related incident at the HFEA office could result in staff being unable to access key services hosted on the Azure Cloud.

EXECUTIVE SUMMARY

1. Next Steps

4.1 To improve the controls on hosting services on a public cloud platform, and the provision of a meaningful report to the Audit and Governance Committee, management are now required to:

- Consider the recommendations made in Section 3; and
- Complete Section 5 (Recommendations Table: Agreed Action Plan) detailing what action you are intending to take to address the individual recommendations, the owner of the planned actions and the planned implementation date.

4.2 The agreed action plan will then form the basis of subsequent audit activity to verify that high priority recommendations have been implemented effectively and for management to monitor implementation of all recommendations.

4.3 If management do not accept any of the recommendations made then a clear reason should be provided in the action plan.

4.4 Finally, we would like to thank management for their help and assistance during this review.

FINDINGS/OBSERVATIONS

2. Recommendations

Customer to provide details of planned action; owner and implementation date. Action taken will later be assessed by Health Group Internal Audit, and therefore the level of detail provided needs to be sufficient to allow for the assessment of the adequacy of action taken to implement the recommendation to take place.

№	RATING	RECOMMENDATIONS	MANAGEMENT RESPONSE	AGREED ACTION PLAN: OWNER & PLANNED IMPLEMENTATION DATE
1.	**L**	**Cloud lock-in** - we recommend HFEA to update their Change Management policies to ensure cloud lock-in is considered before any cloud related change occurs such as the introduction of new infrastructure. This will reduce the likelihood of HFEA being locked-in with Microsoft Azure in the future.	Agreed. Cloud lock in will be considered in advance of selection of any PAAS products.	Head of IT. In place
2.	**L**	**Business Continuity** - We recommend HFEA to update their Business Continuity policies to ensure it has appropriate plans and procedures in the event of an incident, such as network failure impacting services hosted on the Azure Cloud. This could be something simple as allowing staff to work from a secure environment such as their home via a secure VPN connection.	Agreed. IT staff can already access Azure services from remote locations. General HFEA staff can access Office 365 from home. We will investigate divergent route network connectivity for Spring Gardens.	Head of IT Remote access in place. Divergent route to be investigated by end of April.

APPENDIX

Appendix A – Priority and Report Rating Definitions

Priority Rating - Definitions

Priority	Description
HIGH	Fundamental weaknesses in control which expose the Accounting Officer / Director to high risk or significant loss or exposure in terms of failure to achieve key objectives, impropriety or fraud. Senior managers are expected to oversee the prompt implementation of agreed actions, or to confirm in writing that they accept the risks of not implementing a high priority internal audit recommendation.
MEDIUM	Significant weaknesses in control, which, although not fundamental, expose the Accounting Officer / Director to a risk of loss, exposure or poor value for money. Managers are expected to oversee the prompt implementation of agreed actions, or to confirm in writing that they accept the risks of not implementing a medium priority internal audit recommendation. Failure to implement recommendations to mitigate these risks could result in the risk moving to the High category.
LOW	Minor weakness in control which expose the Accounting Officer / Director to relatively low risk of loss or exposure. However, there is the opportunity to improve the control environment by complying with best practice. Suggestions made if adopted would mitigate the low level risks identified.

Report Rating – Definitions

Rating	Description
SUBSTANTIAL	In Internal Audit's opinion, the framework of governance, risk management and control is adequate and effective.
MODERATE	In Internal Audit's opinion, some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
LIMITED	In Internal Audit's opinion, 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	In Internal Audit's opinion, 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.

APPENDIX

Appendix B - Cloud workshop findings:

The review was delivered via a workshop, where industry specialists with management determined the business impact and likelihood of potential risks. This outcome of the workshop provided management with a prioritised list of high, medium and low cloud security risks relevant to HFEA's IT environment. Each risk was given a value for Business Impact (low to high - 0 to 4) and a likelihood of it occurring (low to high – 0 to 4).

This risk scale was mapped to a simple overall risk rating according to the overall score of the risk for business impact and likelihood of it occurring:

3.1. Low risk: 0-2;
3.2. Medium Risk: 3-5; and
3.3. High Risk: 6-8.

Management provided evidence of actual controls in place for risks rated medium or above. Recommendations were provided when there was a requirement to enhance the adequacy and effectiveness of HFEA's controls for their infrastructure hosted in the Cloud.

Note: Microsoft's Service Trust Portal provides independently audited compliance reports for the Azure Cloud platform as evidence of all their certifications including G-Cloud and ISO27001.

APPENDIX

	Risk	Business Impact	Likelihood	Risk Rating (0-8)	Expected Control	Actual Control
Policy and Organisational Risk	Cloud Lock-in	2	1	3	Appropriate planning has taken place to ensure HFEA will not be locked into the Azure platform. An exit strategy from the Azure Cloud should also exist.	HFEA's **Detailed Architecture** document shows the infrastructure has been designed to ensure there is not a reliance on the Microsoft Azure Cloud platform. However, we recommend HFEA to update their Change Management policies to ensure cloud lock-in is considered before any cloud related change occurs such as the introduction of new infrastructure. This will reduce the likelihood of HFEA being locked-in with Microsoft Azure in the future (see Finding 1).
	Loss of security governance	4	1	5	Microsoft Azure Cloud have appropriate physical and logical security controls.	Microsoft Azure have appropriate physical and logical security controls. They are **ISO27001** certified for their implementation of information management security standards, which cover physical and logical security controls. In addition, Microsoft Azure adheres to the UK government initiative **Government Cloud (G-Cloud)**. It has been created to ease procurement of cloud services by government departments and promote government-wide adoption of cloud computing. G-Cloud comprises a series of framework agreements including physical and logical security. They also have **ISO 27017** certification as Microsoft cloud services have implemented this Code of Practice for Information Security Controls.
	Supply chain failure	4	0	4	The contract with the cloud provider such as Azure ensures they are responsible for maintaining Service Level Agreements and Security policies rather than any third parties they engage with.	Microsoft Azure adheres to the **UK Government's G-Cloud certification**, which includes appropriate supply chain security *(The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement).* Microsoft Azure also adheres to **ISO 22301** for its implementation of these business continuity management standards.
	Conflicts between HFEA hardening procedures and cloud environment	1	1	2	Microsoft Azure Cloud's information security policies have been reviewed to ensure they align with HFEA's.	N/A

APPENDIX

	Risk	Business Impact	Likelihood	Risk Rating (0-8)	Expected Control	Actual Control
Technical Risk	Resource exhaustion	4	0	4	Cloud service agreements and service level expectations terms and conditions are reasonable, verifiable and do not conflict with business requirements.	HFEA's **contract** with Microsoft Azure has appropriate T&Cs to ensure Microsoft adhere to an expected level of service.
	Isolation failure	4	0	4	Although Azure logically separate tenant data, in the unlikely instance HFEA data is compromised, it is encrypted at rest to reduce the impact of the isolated failure.	Microsoft Azure adheres to the UK government initiative **Government Cloud (G-Cloud)**. It has been created to ease procurement of cloud services by government departments and promote government-wide adoption of cloud computing. G-Cloud comprises a series of framework agreements with cloud services suppliers and includes Separation between consumers (Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another). Microsoft Azure is **ISO27018** certified - Microsoft was the first cloud provider to adhere to this code of practice for cloud privacy.
	Cloud provider abuse of high privilege roles	4	1	5	The Cloud provider has appropriate information security policies and staff vetting procedures (e,g criminal and financial background checks) to reduce the likelihood of individuals abusing high privilege roles.	Microsoft Azure have appropriate physical and logical security controls. The service provider is **ISO27001** certified for their implementation of information management security standards, which cover physical and logical security controls. In addition, Microsoft Azure adheres to the UK government initiative **Government Cloud (G-Cloud)**. This includes having appropriate controls for personnel security such as staff vetting and training.
	Management interface compromise	4	1	5	Appropriate controls are in place to ensure Microsoft Azure's Cloud management portal is not easily accessible and limited individuals from HFEA have access to it.	As Microsoft Azure adheres to the UK **Government's G-Cloud certification**, which includes having appropriate External interface protection (All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them). HFEA also have a permission matrix as well as a password policy within the **Information Security Policies document**.

APPENDIX

	Risk	Business Impact	Likelihood	Risk Rating (0-8)	Expected Control	Actual Control
	Interception of data in transit	4	1	5	Data in transit is encrypted to reduce the impact of data being intercepted when being transferred from different sites (via the internet).	Microsoft Azure adheres to the UK **Government's G Cloud certification**, which includes Data in Transit Protection (Consumer data transiting networks should be adequately protected against tampering and eavesdropping (confidentiality)).
	Insecure or ineffective deletion of data	4	0	4	Microsoft Azure Cloud keeps deleted data for 90 days, which can be recovered within that time period. HFEA need to ensure the number of individuals with access to this data is very limited.	Microsoft Azure is **ISO27018** certified, the international code of practice for cloud privacy (*After this 90-day retention period, Microsoft will disable the account and delete the customer data, including any cached or backup copies. For in-scope services, that deletion will occur within 90 days after the end of the retention period).* In addition, Microsoft Azure adheres to the UK government initiative **Government Cloud (G-Cloud)**. This includes Asset Protection *(when customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before reuse. As part of agreements for cloud services such as Azure Storage, Azure VMs, and Azure Active Directory, Microsoft contractually commits to timely deletion of data. Upon a system's end-of-life, Microsoft operational personnel follow rigorous data handling procedures and hardware disposal processes to help assure that no hardware that may contain customer data is made available to untrusted parties).*
	Distributed denial of service (DDoS)	2	2	4	HFEA have appropriate controls to ensure the impact of a DDoS is limited.	HFEA have provided **Web Configuration** evidence that the service hosted on Microsoft Azure is limited to 20 requests at any one time. Therefore, HFEA have appropriate controls to ensure the impact of a DDoS attack is very limited.
	Compromise of service engine	2	0	2	In the event of Microsoft Azure's service engine being compromised, HFEA's data is encrypted to ensure minimal impact.	N/A

APPENDIX

<table>
<tr><th></th><th>Risk</th><th>Business Impact</th><th>Likelihood</th><th>Risk Rating (0-8)</th><th>Expected Control</th><th>Actual Control</th></tr>
<tr><td></td><td>Loss of cryptographic keys</td><td>3</td><td>1</td><td>4</td><td>HFEA have appropriate cryptographic keys governance policies to limit the likelihood in the loss of cryptographic keys.</td><td>HFEA also have a Password permission matrix as well as a password policy within the Information Security Policies document.

Microsoft Azure have appropriate physical and logical security controls. They are ISO27001 certified for their implementation of information management security standards, which cover physical and logical security controls.

In addition, Microsoft Azure adheres to the UK government initiative Government Cloud (G-Cloud) comprising a series of framework agreements including physical and logical security.</td></tr>
<tr><td></td><td>Non cloud-specific network-related technical failures or attacks</td><td>1</td><td>4</td><td>5</td><td>HFEA have a secondary network link with a different network provider to reduce the likelihood of network failure, which will impact access to the Azure platform.</td><td>HFEA have a Business Continuity policy. However, we recommend HFEA to further update their Business Continuity policies to ensure it has comprehensive plans and procedures in the event of an incident, such as network failure impacting services hosted on the Azure Cloud. This could be something simple as allowing staff to work from a secure environment such as their home via a secure VPN connection (see Finding 2).</td></tr>
<tr><td></td><td>Loss of backups</td><td>4</td><td>1</td><td>5</td><td>Adequate IT Disaster Recovery arrangements have been established to enable HFEA to recover from significant disruption to IT systems or services such as secondary backups.</td><td>SQL Databases on Microsoft Azure have several business continuity features, including automated backups and optional database replication. For Release 1 HFEA have chosen the below (ERT - estimated recovery time and RPO – Recovery Point Objective) :

Standard tier<table><tr><th>Point in Time Restore from backup</th><th>Any restore point within 35 days</th></tr><tr><td>Geo-Restore from geo-replicated backups</td><td>ERT < 12h, RPO < 1h</td></tr><tr><td>Restore from Azure Backup Vault</td><td>ERT < 12h, RPO < 1 wk</td></tr><tr><td>Active Geo-Replication</td><td>ERT < 30s, RPO < 5s</td></tr></table>NOTE: Business Continuity features for Release 2 have yet to be chosen.</td></tr>
</table>

APPENDIX

	Risk	Business Impact	Likelihood	Risk Rating (0-8)	Expected Control	Actual Control
	Natural disasters	2	1	3	Adequate IT Disaster Recovery arrangements have been established to enable HFEA to recover from significant disruption caused by natural disasters.	Microsoft Azure adheres to the UK government initiative **Government Cloud (G-Cloud)** compromising a series of framework agreements including resilience.
Legal Risk	Data protection	2	1	3	HFEA still adheres to Data Protection Laws - data is hosted within the EU.	In our review, we have considered the requirements of the General Data Protection Regulation (GDPR), which will be applicable from 25 May 2018. According to the **Detailed Architecture** document, the current location of the Azure data centres used do not pose a compliance issue as they are within the European Economic Area. The Release 2 detailed architecture document confirms this.
	Licensing issues	0	1	1	HFEA are aware of any licence requirements they still have, although the particular infrastructure is hosted on the public cloud.	N/A
	Intellectual property	1	1	2	Appropriate contracts are in place to ensure HFEA always own the intellectual property, even though their services are hosted on their public cloud servers.	N/A