Audit and Governance Committee meeting - agenda

21 March 2017

Abbey Room

Church House Westminster, Dean's Yard, Westminster SW1P 3NZ

Agenda item			Time
1.	Welcome, apologies and declaration of interests		09:45am
2.	Minutes of 7 December 2016 **[AGC (21/03/2017) 523]**	For Decision	10.00am
3.	Matters Arising **[AGC (21/03/2017) 524 MA]**	For Information	10.05am
4.	Internal Audit		10.15am
	a) Introduction to HIA **[AGC (21/03/2017) 525 DH]**	Verbal Update	
	b) Internal Audit Progress Report **[AGC (21/03/2017) 526 DH]**	For Information	
	c) Board Effectiveness – Final Report **[AGC (21/03/2017) 527 DH]**	For Discussion	
	d) Information Standards – Final Report **[AGC (21/03/2017) 528 DH]**	For Discussion	
	e) Implementation of Recommendations **[AGC (21/03/2017) 529 MA]**	For Information	
	f) Cloud Cyber Risk Assessment (advisory audit) **[AGC (21/03/2017) 530 DH]**	For Information	
	g) Final report and annual opinion* **[AGC (21/03/2017) 531 DH Internal Audit]**	Verbal update	
5.	External Audit – Interim Feedback **[AGC (21/03/2017) 532 NAO]**	Verbal Update	10.45am
6.	Finance and Resources Update **[AGC (21/17/2017) 533 RS]**	Presentation	10.50am
7.	Information Governance Group Activities **[AGC (21/17/2017) 534DM]**	Verbal	11.10am
8.	Cyber Security **[AGC (21/17/2017) 535DM]**	For Information	11.25am

9.	Resilience & Business Continuity Management **[AGC (21/17/2017) 536 DM]**	For Information	11.30am
10.	AGC Forward Plan **[AGC (21/03/2017) 537 MA]**	For Decision	11.55am
11.	Strategic Risk Register **[AGC (21/03/2017) 538 PR]**	For Information/Comment	12.05pm
12.	Information for Quality (IfQ) Programme **[AGC (21/03/2017) 539 NJ]**	For Information	12.15pm
13.	Whistle Blowing and Fraud **[AGC (21/03/2017) 540 RS]**	Verbal update	12.25pm
14.	Contracts and Procurement **[AGC (21/03/2017) 541 MA]**	Verbal update	12.30pm
15.	Any other business		12.35pm
16.	Close (Refreshments & Lunch provided)		12.40pm
17.	Session for members and auditors only		12.40pm

18. Next Meeting 10am Tuesday, 13 June 2017, London

*Report due on completion of all audits.

Human Fertilisation & Embryology Authority

Audit and Governance

Committee meeting minutes

Strategic delivery:	☐ Setting standards	☐ Increasing and informing choice	☐ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item	2		
Paper number	AGC (21/03/2017) 523		
Meeting date	21 March 2017		
Author	Dee Knoyle, Committee Secretary		
Output:			
For information or decision?	For decision		
Recommendation	Members are asked to confirm the minutes as a true and accurate record of the meeting		
Resource implications			
Implementation date			
Communication(s)			
Organisational risk	☐ Low	☐ Medium	☐ High
Annexes			

Minutes of Audit and Governance Committee meeting held on 7 December 2016 at King's College London, Strand Campus, Strand, London WC2R 2LS

Members present	Rebekah Dundas (Chair) Anita Bharucha Margaret Gilmore Gill Laver Jerry Page (Teleconference)
Apologies	None
External advisers	Government Internal Audit Agency (GIAA): Jon Whitfield Internal Audit - PricewaterhouseCoopers (PwC): Karen Finlayson Paul Foreman External Audit - National Audit Office (NAO): Sarah Edwards George Smiles
Observers	None
Staff in attendance	Peter Thompson, Chief Executive Richard Sydee, Director of Finance & Resources Morounke Akingbola, Head of Finance Wilhelmina Crown, Finance & Accounting Manager Nick Jones, Director of Compliance and Information David Moysen, Head of IT Paula Robinson, Head of Business Planning Siobhain Kelly, Interim Head of Corporate Governance Dee Knoyle, Committee Secretary

1. Welcome, apologies and declarations of interests

1.1 The Chair welcomed attendees to the meeting, in particular:

- Richard Sydee, the new Director of Finance & Resources for the HFEA and HTA, attending his first Audit and Governance Committee meeting.
- Jon Whitfield from the Government Internal Audit Agency (GIAA)

1.2 Kim Hayes, Department of Health was unable to observe this meeting and sent her apologies.

1.3 There were no declarations of interest.

2. Minutes of the meeting held on 21 September 2016

2.1 The minutes of the meeting held on 21 September 2016 were agreed as a true record of the meeting and approved for signature by the Chair with the amendment of the meeting date at point 2 and 2.1.

2.2 Margaret Gilmore notified members that since the last meeting she has agreed to continue her support to the Audit and Governance Committee but will no longer sit on the Licence Committee.

3. Matters arising

3.1 The committee noted the progress on actions from previous meetings. Some items were ongoing and others were dependent on availability or were planned for the future.

3.2 e) Since the two external members have been provided with the dates for future Authority meetings, and have had them for some time, it was agreed that this item would be marked as complete.

3.3 9.6) The Director of Finance & Resources will provide an update on the Information Governance Group activities at the next Audit and Governance Committee Meeting.

3.4 12.6) Due to the untimely departure of the former Head of Governance, the review of the Appeals process has been delayed.

3.5 14.5) The Executive are still awaiting the Triennial review report.

3.6 5.7) The Information for Quality (IfQ) Internal Systems Project Manager will circulate a list of recommendations and planned actions (relating to ‘Public Beta’) to the committee after review by Programme Board. The Director of Compliance and Information to follow up.

3.7 Item 4.11, 5.20 and 5.21 have been addressed in the items on the agenda below.

3.8 The Chair thanked the Finance Team for their efforts and was pleased to see that some progress had been made.

4. Rating

4.1 Jon Whitfield, Head of Government Internal Audit, Government Internal Audit Agency (GIAA) provided the committee with a briefing on the internal audit rating system.

4.2 The rating of audit reports has four tiers, substantial, moderate, limited and unsatisfactory.

4.3 The committee noted that the HFEA received a moderate rating for its audit report. The moderate rating means that, in internal audit opinion, some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.

4.4 The committee was informed that 90% of all public sector organisations have received a rating somewhere in the middle.

4.5 The committee was concerned that some recommendations were not applicable to the size and nature of the organisation and therefore implementation would be inappropriate and burdensome on such a small Arm’s Length Body. The committee was also concerned about the public perception of the HFEA receiving a moderate rating.

4.6 Jon Whitefield highlighted that he encouraged internal auditors to be bolder in their opinions that accompany the rating, in order to put it into context.

5. Register & Compliance

5.1 The Director of Compliance and Information provided the committee with a briefing and a presentation on the directorate's risks.

5.2 The committee was reminded of the directorate's role and responsibilities. The committee was also provided with an update on the directorate's achievements since this item was last presented to the committee in 2015.

5.3 The committee noted that most of the staff in this directorate are juggling business as usual alongside the Information for Quality (IfQ) programme. Staff from the Information Team and the IT team have been heavily involved in the programme which involves the development of the new clinic portal, website and the Choose a Fertility Clinic online application. The IT team are also responsible for cyber security and work has increased with the migration of data from the HFEA servers to the Cloud storage system.

5.4 The committee was informed that Sharon Fensome-Rimmer, the new Chief Inspector who started in May 2016, has settled in and is working with the team. Sharon brings an awful lot of competence and experience relating to Quality Management Systems and best practice approach to audit, particularly learning lessons from incidents from non-compliances and is a good addition to the team. The inspection programme over the last year has been challenging, however this has been made more achievable by coordinating compliance across emerging clinic groups.

5.5 The data held in the HFEA Register has been checked and improved. Information for donors is being managed well amongst a small specialist team and a third party has been contracted to provide a counselling service which is working well.

5.6 HFEA Regulations and the Code of Practice will be updated in April 2017.

5.7 The Licensing of Research projects is currently being reviewed.

5.8 The committee acknowledged that the directorate is working with limited resources and working hard on the IfQ programme whilst continuing with business as usual. The committee agreed that in order to manage the programme people management and change management will need to be handled well with a shared understanding of the consequences of change. The committee agreed that they must see benefits realisation of the IfQ programme.

5.9 The committee was pleased to hear that the directorate had managed a challenging programme of inspections over the last year and encouraged staff to raise the bar and push it further for the planned work ahead.

5.10 The committee noted the risks above tolerance and agreed that they should be closely monitored and action taken where necessary.

5.11 The committee was pleased with the progress to date and reassured that the risks were well managed.

6. Information for Quality (IfQ) Programme

6.1 The Director of Compliance and Information provided the committee with a paper, presentation and briefing.

6.2 The IfQ programme is currently in the closing stages of its 'public beta' phase for both the Clinic Portal and the new Website.

Clinic Portal - Release One

6.3 Release one of the Clinic Portal has delivered all of the key outputs of the project. The Department of Health Government Digital Service (GDS) assessment took place on 21 November 2016 and a full pass assessment was achieved. The team is now preparing to go live and preparing to de-commission the existing Clinic Portal.

Clinic Portal - Release Two – Electronic Patient Record System (EPRS)

6.4 Release two of the Clinic Portal focuses on the treatment data submission system for clinics and the new Register. The Executive has been preparing for release two over the last year, working on the new Register structure, data cleansing and internal systems infrastructure. Work has been slow but steady and progress is being made.

HFEA Website

6.5 A judicial review hearing, relating to how the HFEA plans to present data on the new website, is scheduled in December 2016. This has delayed some aspects of the programme, however the delay is outside of the organisation's control. Should the judicial review have a negative outcome for the HFEA the existing Choose a Fertility Clinic model could be used and the data for this particular clinic could be removed.

6.6 Further adjustments may be made following a review by the HFEA Authority at its meeting on 15 December 2016 and pending the outcome of the judicial review hearing. The service will later undergo a GDS assessment before going to full 'live' service.

6.7 The HFEA Annual Conference will be used to provide an update on progress to stakeholders.

Committee's comments

6.8 The committee was very pleased to hear that the HFEA had passed the GDS assessment for release one of the Clinic Portal and thanked staff involved for their hard work to achieve this.

6.9 The committee had concerns about the judicial review and the delays this has caused. The committee noted the options appraisal and discussed the consequences of investing money for each timeline presented, including delaying work until June 2017, which required no additional resource. The committee noted that a delay to the timeline would impact on the delivery of the EPRS which would impact on the organisation's ability to monitor and manage treatment fees linked to the submission of data, therefore impacting on one of the benefits of the programme. There was a broad ranging discussion, with one member noting that investing additional resources, large or small, still does not guarantee a smooth and successful delivery. The committee agreed that whichever option was taken the Executive should provide clarity on how that decision was made. The Executive should be mindful of any sensitivity with regard to legal cases, manage expectations and the organisation's reputation.

6.10 The committee discussed the risks within the programme, in particular how quickly contractors would get up to speed. The committee was reassured that contractors with the right skill set could be employed to support the programme reasonable quickly.

6.11 The committee noted that the Executive will shortly discuss the budget with the Department of Health.

7. Strategic Risks

7.1 The Head of Business Planning presented the strategic risk register.

7.2 The committee discussed the strategic risks, in particular the three risks above tolerance which include Information for Quality (IfQ3) – delivery of promised efficiencies, Data(D2) – incorrect data release and Capability (C1) – knowledge and capability.

7.3 At the last Audit and Governance Committee meeting in September 2016, the Executive was asked to give more consideration to 'plan B' for the website, in the event of an adverse judicial review judgment, or in the event of Red Dot (the current, outgoing content management system, which was old and unsupported) failing completely. One member requested that the Strategic Risk Register paper presented to the Audit and Governance Committee be edited to clarify that the November Authority meeting discussed strategic risks, in the context of various items on the agenda, particularly the strategic performance report and the IfQ progress report.

7.4 The committee questioned whether the Business Continuity Plan had been tested and was informed that there was an incident involving loss of power at the new HFEA premises in the summer of 2016 and the plan had been put into action. There were some lessons learned but generally things worked well.

7.5 The committee was concerned about the fluctuation of Parliamentary Questions that need to be answered within a tight timeframe and questioned how the organisation manages this area of work. The committee was informed that some questions could be tricky to answer. There is a small team of people in the organisation handling the questions, however sometimes the work is extended to other staff with specialist knowledge to contribute to the answers. Answering parliamentary questions always takes priority in the organisation.

8. Internal Audit

a) Progress Report 2016/17

8.1 The committee was provided with a progress report on the internal audit plan for the year, the terms of reference for Cloud security assessment and a briefing.

8.2 The Board of effectiveness review has been completed and the report is currently in draft and is with the Chair and CEO. The review was positive and above the benchmark. The report will be submitted to the Audit and Governance Committee in March 2017, following a management review.

b) Terms of Reference – Cloud Security Assessment

8.3 The field work on Cyber Risks has been completed and will be discussed at item 11.

9. External audit

9.1 The National Audit Office (NAO) provided the committee with the audit planning report and a briefing.

9.2 Key areas of risk were highlighted:

- expenditure relating to IfQ that is capitalised in year – must meet the recognition criteria as set out on IAS 38 intangible assets.
- new Director of Finance & Resources - loss of corporate knowledge may impact on the operation of the overall controls environment

- Brexit – Timing of Article 50 to be triggered in March 2017 – management to consider any impact on the Financial Statements and disclosures after March 2017.

9.3 The committee pointed out that there was an error in the date for the next Audit and Governance Committee meeting – this will be held on Tuesday, 21 March 2017.

10. Implementations of recommendations progress report

10.1 The Finance & Accounting Manager provided the committee with an update.

10.2 The committee was informed that an audit of the Income Generation was conducted. There were three recommendations made, two of which have been completed and one, due to be completed by the end of December 2016 which has been delayed due to the Information for Quality Programme.

11. Cyber Security

11.1 The Head of IT provided the committee with a paper and briefing on the security and testing of the organisation's IT systems.

11.2 The committee is aware that the organisation is focused on moving its data to the Cloud.

11.3 The committee was informed of the organisation's approach to achieving the necessary assurances for cyber security. This includes assessing security handling, penetration testing and ensuring that its software is fit for purpose. PwC, our internal auditors have provided the Executive with terms of reference for Cloud security assessment and will be working with staff to identify any gaps in the HFEA's information framework.

11.4 The committee noted that all public bodies were required to use DMARC (Domain-based Message Authentication, Reporting & Conformance) for email security from 1 October 2016 and that the Executive has considered this. The Head of IT confirmed that DMARC was in place.

11.5 The committee agreed that regular updates on cyber security should be provided to the Audit and Governance Committee.

Action

11.6 Head of IT to provide the Audit and Governance Committee with regular updates on cyber security.

12. Disclosure and Barring Service (DBS) checks

12.1 The committee was provided with a briefing by the Chief Executive.

12.2 The committee was informed that the Executive had discussed the idea of using the disclosure and barring service, however they did not identify areas where this might be appropriate, as there was no contact with juveniles or vulnerable people.

12.3 The committee agreed that further discussions should take place to conclude whether this would be appropriate in any areas of the organisation.

Action

12.4 Peter Thompson, Chief Executive and Jerry Page, member to hold a discussion on DBS checks to explore this area further.

13. Resilience & Business Continuity Management

13.1 The Head of IT provided the committee with an oral briefing on resilience and business continuity management.

13.2 The committee was informed during a discussion on the Strategic Risk Register that the business continuity plan had been tested. There were areas identified for improvement.

13.3 The committee agreed that lessons learned should be noted and recommendations for action required should be implemented with further testing.

13.4 The committee agreed that an update on resilience and business continuity should be presented to the Audit & Governance Committee at a future meeting.

Action

13.5 Head of IT to provide the Audit and Governance Committee with an update on resilience and business continuity at a future meeting.

14. Whistle Blowing Policy

14.1 The Head of Finance provided the committee with the Whistleblowing policy and a briefing.

14.2 The committee was guided through the small amendments to the policy.

14.3 The committee noted that the policy has not been used by any member of staff in the last 10 years and questioned whether or not staff know about it. The committee was informed that the policy is available to staff on the internal intranet and changes are announced at meetings organised for all staff.

14.4 The committee asked for clarification on point 6.4 relating to the provision of information for individuals raising concern. The committee wanted to know whether confirmation that the individual is entitled to independent advice was applicable. This will be further investigated.

Action

14.5 Head of Human Resources to provide clarification on point 6.4 of the policy, confirming whether individuals raising concern are entitled to independent advice.

15. Contracts & Procurement

15.1 There was a tender for animation for the new HFEA website in September 2016 for approximately £8000.

16. Review of AGC activities & effectiveness

16.1 The Interim Head of Corporate Governance provided the committee with the NAO checklist.

16.2 The committee's comments and suggestions were collated and will be sent to the committee for comments.

16.3 The internal auditors notified the committee that there is a later version of the checklist available. However the committee was happy to use the version provided by the NAO.

16.4 The committee commented that it was also appreciative of the work that goes into preparing for the meeting and papers received.

17. AGC Forward plan

17.1 The committee was satisfied with the content of the Forward Plan of agenda items for the forthcoming meetings.

17.2 The committee agreed that future discussions should focus on more long term risks and the Executive should think about areas which may have lost priority due to the focus on the Information for Quality Programme.

18. Any other business

18.1 This is the last meeting to be attended by the Chair, Rebekah Dundas who will be leaving the Authority at the end of December 2016 after 10 years of service. Rebekah thanked attendees for their contributions to the meetings and thanked the Executive for all of their hard work and support for the Audit and Governance Committee meetings during her time as Chair.

18.2 The Deputy Chair thanked Rebekah, on behalf of the members and the Executive for supporting the HFEA in her role as Chair of the Audit and Governance Committee.

18.3 Members and auditors retired for their confidential session.

18.4 The next meeting will be held on Tuesday, 21 March 2017 at 10am.

Chair’s signature

18.5 I confirm this is a true and accurate record of the meeting.

Signature

Name

Anita Bharucha on behalf of Rebekah Dundas

Date

21 March 2017

Audit and Governance Committee Paper

Paper Title:	**Matters arising from previous AGC meetings**
Paper Number:	**[AGC (21/03/2017) 524 MA]**
Meeting Date:	21 March 2017
Agenda Item:	**3**
Author:	Morounke Akingbola, Head of Finance
For information or decision?	Information
Recommendation to the Committee:	To note and comment on the updates shown for each item.
Evaluation	To be updated and reviewed at each AGC.

Numerically:

- 3 items added from December 2016 meeting, 2 ongoing
- 4 items carried over from earlier meetings, 4 ongoing

Matters Arising from Audit and Governance Committee – actions from 10 June 2015 meeting			
ACTION	**RESPONSIBILITY**	**DUE DATE**	**PROGRESS TO DATE**
9.6 Report progress on actions from the information governance group to AGC	Director of Finance and Resources	December 2016	**Ongoing** – The Director of Finance & Resources will provide an update on the Information Governance Group activities at the next Audit and Governance Committee Meeting in March 2017.
Matters Arising from Audit and Governance Committee – actions from 9 December 2015 meeting			
ACTION	**RESPONSIBILITY**	**DUE DATE**	**PROGRESS TO DATE**
12.6 The Executive to add a review of the procedures for representations to the Business Plan for 2016/17 and report back to the Authority with recommendations, in due course.	Head of Business Planning	April 2016	**Ongoing -** Was added to 16/17 business plan. Confirmation as to whether review was conducted to be received.
14.5 The Triennial review report is to be sent to committee members.	Director of Finance	When published	**Ongoing –** The Executive are still awaiting the Triennial review report.
Matters Arising from Audit and Governance Committee – actions from 15 June 2016 meeting			
5.7 Circulate a list of recommendations and planned actions (relating to public beta) to the committee after review by Programme Board	Information for Quality (IfQ) Internal Systems Project Manager	January 2017	**Ongoing -** Due to staff changes and lapse of time, request for this to be removed.
Matters Arising from Audit and Governance Committee – actions from 7 December 2016 meeting			
11.6 Head of IT to provide the Audit and Governance Committee with regular updates on Cyber Security.	Head of IT		**Ongoing –** Agenda item for March 2017 meeting
13.5 Head of IT to provide the Audit and Governance Committee with an update on resilience and business continuity at a future meeting,	Head of IT	March 2017	**Completed** – Agenda item for March 2017 meeting

14.5 Head of Human Resources to provide clarification on point 6.4 of the policy, confirming whether individuals raising concern are entitled to independent advice.	Head of Human Resources		**Ongoing –** Clarification is sort from the Committee as to what they really mean. We do not stop people from seeking advice from third parties such as HSE or a Professional Institute.

Health Group Internal Audit

INTERNAL AUDIT PROGRESS REPORT MARCH 2017

Health Group Internal Audit provides an objective and independent assurance, analysis and consulting service to the Department of Health and its arm's 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 arm's 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.

For further information please contact:
Cameron Robson - 01132 54 6083
1N16 Quarry House, Quarry Hill,
Leeds, LS2 7UE

Our work has been conducted and our report prepared solely for the benefit of the Department of Health and its arm's length bodies and in accordance with a defined and agreed terms of reference. In doing so, we have not taken into account the considerations of any third parties. Accordingly, as our report may not consider issues relevant to such third parties, any use they may choose to make of our report is entirely at their own risk and we accept no responsibility whatsoever in relation to such use. Any third parties, requiring access to the report may be required to sign 'hold harmless' letters.

CONTENTS **PAGE**

1. Introduction 1

2. Progress against 2016/17 Internal Audit Plan 1

2.1 Status of agreed plan 1

2.2 Summary of reports issued since the last Audit and Governance Committee 3

2.3 Follow up work 3

2.4 Impact on Annual Governance Statement 4

Appendix 1: Report Rating Definitions 5

Appendix 2: Limitations and responsibilities 6

HFEA Internal Audit Progress Report March 2017

1) Introduction

This paper sets out the progress in completing the 2016/17 Internal Audit Plan since the last meeting of the Audit and Governance Committee in December 2016.

2) Progress against 2016/17 Internal Audit Plan

2.1 Status of agreed plan:

The table below summarises the progress against each of the review areas in the 2016/17 Audit Plan:

Reviews per 201/17 IA plan	Audit scope	Status	Findings			Overall report rating	Audit days per plan	Actual audit days
			High	Medium	Low			
Income generation process	These reviews were merged into one as they both focused on the revenue process. We mapped the income generation and invoicing process from receipt of the electronic treatment forms from clinics to the raising of an invoice. In addition, we evaluated the design and operating effectiveness of controls over the data being used within the income process, considering the mechanisms to ensure that the original source data is of appropriate quality to support invoicing and the checks in place to ensure that integrity of data is maintained during the income and invoicing process. Management also requested that we review the risk management process in place in	Final report issued	0	1	4	**Moderate**	5	9
Quality and efficiency of revenue data							4	

Reviews per 201/17 IA plan	Audit scope	Status	Findings			Overall report rating	Audit days per plan	Actual audit days
			High	Medium	Low			
	relation to the transition of income processing to the Integrated Clinic Portal.							
Information standards	As NHS England are assessing the information governance arrangements of HFEA's patient oriented information to ensure published information is up to date and accurate, it was agreed that our work should focus on the application of the policy to corporate information.	Final report issued	0	1	2	Moderate	5	5
Board effectiveness	This was a high level review to assess the Board effectiveness via a self-assessment survey and follow-up interviews.	Final report issued	0	0	2	Not rated	6	7
Management of Cyber Penetration threat	Following scoping discussions with the Head of IT, it was agreed that this workshop would focus on identifying security risks relating to a cloud environment and identifying any gaps in HFEA's security control framework. The workshops were delivered in February 2017.	Draft report issued 6 March	0	0	2	Moderate	5	5
Assurance mapping	This time was assigned in the plan for an assurance mapping workshop. However, it was agreed with the Audit and Governance Committee to hold the resource for possible need to give further consideration to Cyber Security, that being dependent on the outcome of the initial work in that area as outlined above.	Scope to be determined.				Not applicable	3	0
Audit Management	All aspects of audit management to include: • Attendance at liaison meetings and HFEA Audit and Governance	Ongoing	Not applicable			Not applicable	7	7

Reviews per 201/17 IA plan	Audit scope	Status	Findings			Overall report rating	Audit days per plan	Actual audit days
			High	Medium	Low			
	committees; • Drafting committee papers/progress reports; • Follow-up work; • Resourcing and risk management; and • Contingency.							
Contingency							5	-
		Total Findings:	0	1	4			
						Total days	40	33

2.2 Summary of reports issued since the last Audit and Governance Committee:

Since the last Audit and Governance Committee in December 2016 we have issued final reports on Board Effectiveness and Information Standards. These reports accompany this progress paper.

2.3 Follow-up work:

The HFEA performs its own follow-up work, reviewing the status of agreed audit actions and reporting progress to the Audit and Governance Committee.

As such, Internal Audit has been asked to provide independent assurance of the completion of agreed actions only over those actions which relate to high priority recommendations. This approach was agreed with the former Director of Finance and Resources.

No high priority actions have resulted from us undertaking the 2016/17 audit reviews to date and none were outstanding at the start of the year from previous audit work. Accordingly, there have been no outstanding high priority recommendations requiring internal audit follow-up work in the year to date.

2.4 Impact on Annual Governance Statement:

All reports issued with an overall Limited or Unsatisfactory rating, or with report findings that are individually rated high priority, should be considered for their possible impact on the Authority's Annual Governance Statement (AGS). To date, no Limited reports and no high priority issues have been raised as a result of us completing the work forming part of the 2016/17 audit plan and all actions relating to previous high priority issues have been completed. Accordingly, there are currently no matters arising from our work to date that we believe may require reference in the AGS.

Appendix 1 – Report Rating Definitions

Priority Ratings of individual findings:

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.

Ratings of audit reports

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 2 - Limitations and responsibilities

Internal control

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

Future periods

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 operating environment, law, regulation or other; or
- the degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems. We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected. Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.

Health Group Internal Audit

Reference number: DH216008004
FINAL REPORT
Human Fertilisation and Embryology Authority
February 2017

Report Name: Board Effectiveness Self-Assessment

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.

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

Our work has been conducted and our report prepared solely for the benefit of the Department of Health and its arms length bodies and in accordance with a defined and agreed terms of reference. In doing so, we have not taken into account the considerations of any third parties. Accordingly, as our report may not consider issues relevant to such third parties, any use they may choose to make of our report is entirely at their own risk and we accept no responsibility whatsoever in relation to such use. Any third parties, requiring access to the report may be required to sign 'hold harmless' letters.

CONTENTS PAGE

1.	Introduction	1
2.	Review Conclusion	1
3.	Summary of Findings	2
4.	Next Steps	4
5.	Recommendations Table	5
6.	Findings and Observations	6
	Appendix 1 – Summary of Survey Results	8
	Appendix 2 – Risk and Report Ratings	11

Date fieldwork completed:	8 November 2016
Feedback meeting	23 November 2016
1st draft report issued:	29 November 2016
Management responses received:	3 February 2017
2nd draft report issued:	6 February 2017
Management responses received:	9 February 2017
Final report issued	20 February 2017

Report Author: Lenka Marvanova
Version №: Final v1

Distribution List – Draft Report

Main recipient(s)

Sally Cheshire	Chair

Cc(s)

Morounke Akingbola	Head of Finance
Peter Thompson	Chief Executive
Cameron Robson	Group Chief Head of Internal Audit

Distribution List – Final Report

As above

EXECUTIVE SUMMARY

1. Introduction

1.1 Within the context of an organisation’s purpose, the board has a key role in setting strategy and developing and implementing action plans to achieve objectives. It also has the vital role of monitoring performance and challenging management where that might be improved. An effective board is a key part of governance, risk management and assurance arrangements as well as contributing to the development and promotion of the collective vision of the organisation’s purpose, culture, values and the behaviours. There needs to be effective engagement between independent members and the executive to lead the organisation, whilst avoiding the board becoming too operational and focused on decisions and actions that should be the responsibility of management.

1.2 The Human Fertilisation and Embryology Authority (HFEA) is an Executive non-Departmental Public Body sponsored by the Department of Health. The Chair and the Authority members are appointed by the Secretary of State for Health. The board has 12 members in total, with the Chair, Deputy Chair and at least half of the HFEA members being lay members. While the structure has not changed, board membership has undergone some change during 2016, with two new members appointed in January and February 2016 in place of those whose terms of office had expired. Further changes to the board will take place in Quarter 3 and Quarter 4 of the current financial year. The Authority celebrated 25 years of existence in September 2016.

1.3 Supporting the board, the HFEA has seven committees: Audit and Governance; Remuneration; Appeals; Appointments; Licence; Statutory Approvals; and the Scientific and Clinical Advances Advisory Committee. There are also three panels: Executive Licencing; Register Research; and the Horizon Scanning Panel. The focus of this review has been on the effectiveness of the board, using a self-assessment questionnaire and benchmarking. We have not covered the operation of these other committees and panels.

1.4 The objective of this review was to consider the effectiveness of the HFEA board by undertaking the following:

- Carrying out a self-assessment (via an on line survey) completed by each board member,
- Analysis of the results of the survey (based on the collective results),
- Benchmark the results against other organisations including other Arms’ Length Bodies (ALBs), and
- Undertaking targeted interviews with all board members, informed by the output of the self-assessment questionnaire.

1.5 Our work was performed during October / November 2016.

2. Review Conclusion

2.1 The findings in this report are based on the survey results and follow-up discussions only. The work is intended to help the Chair and the board to further enhance the effectiveness of how the board operates through self-assessment and benchmarking. As result, no assurance conclusion is included in this report.

2.2 The combined results of the board self-assessment and interviews did not identify any significant weaknesses that may impact on the board operating effectively. Indeed, in the view of the Authority board members the board is operating effectively as shown by them rating the HFEA board higher than other organisations included within the benchmarking across all areas assessed.

3. Summary of Findings

3.1 Our review has identified a number of areas of good practice which have been highlighted below, and only a small number of areas for consideration where there may be scope to further enhance the operating effectiveness of the board.

3.2 The average results from the board effectiveness survey have been summarised in Appendix 1. The overall average result for the survey was 5.50 (on scale 1-6 with 6 being the most positive rating), which is a strong indication that the overall effectiveness and operation of the board is viewed as positive by the board members. Indeed, as mentioned above they have rated the HFEA board on average higher than members of each of our comparative boards rated their own organisations.

3.4 Lower than average results were received in the following categories, Of the 12 categories, the following 4 were rated the lowest, although all of these still rated above 5 which is in agreement with the statements of effectiveness in our survey:

- Composition and Structure (5.38)
- Role Clarity (5.42)
- Individual and Whole Board (5.33)
- Development and Succession Plans (5.11)

3.5 Benchmarking the results indicated that the HFEA board is consistently assessed to be performing above the benchmark average in all categories. The benchmarking exercise shows that the Authority received the top score across all categories with an overall score 9.72 points above the benchmark and gap of 5.08 points on the next highest assessed organisation (for the benchmarking exercise, the average score of all responses has been denoted as 100 points, with organisations performing either below or above this benchmark). The results of the benchmarking exercise are also included in the Appendix 1.

3.6 The survey and interview results highlighted board members' concerns about ensuring corporate memory and experience of the board is maintained in the future as the board membership is refreshed in the coming months, with experienced board members having left in September 2016 and in January 2017. Concerns were raised about the requirement to refresh the board membership every three years notwithstanding the benefit of fresh perspectives given the role of members in regulatory decision-making, and while the board members expressed confidence that the appointment process is well managed, they were clearly aware of the risks associated with the potential loss of corporate memory and experience. Those concerns were reflected in the score and feedback provided for two of the survey categories (Composition and Structure, Development and Succession Plans). The concerns regarding length of appointment have been recognised by the HFEA and are part of discussions with the Department of Health, however we are aware that the ultimate responsibility for appointments lies with Cabinet Office and therefore HFEA are limited in actions they can take to address this concern. We understand that the Chair is in discussion with the Department of Health about seeking alternative appointment periods that would enable the organisation to address the concerns already identified. Therefore, we have not raised any recommendations in this respect, but we recognise that pending any agreement with the Department of Health, HFEA will need to continue to focus on managing succession and ensuring robust induction of new board members.

3.7 During the interviews, observations were also made about the workload and demand on time associated with the board members' duties at both the board and the various committees and groups. We understand that determining the size of the board membership is outside HFEA's control, and also that the organisation regulates an industry where developments in research and technology is rapid. This increases demand on the board members time and dealing with the complexities of the decision-making process, all of which highlights the importance of retaining robust corporate memory, experience and expertise and making clear to new members what the expectations are, including between meetings.

3.8 During our review of the survey results and interviews we noted a number of positive comments about the board's effectiveness:

- **Relationships** – we received a number of comments about the positive relationships and working environment at the board meetings and between the board members and the Executive, which is seen to lead to open and diverse discussions. The comments also confirmed that the board operates in a professional environment and is seen to provide an appropriate level of challenge to the Executive team, but in a positive atmosphere. Comments were also received on the cohesiveness of the board, and transparency in decision making.
- **Chair** – both the survey and the interviews indicated the view that the Chair is very effective in managing the board meetings, setting the right tone and encouraging positive and open discussions. The work of the Chair was also seen as pivotal to securing a good mix of skills and experience at the board.
- **Board decision making –** The board has an informal mentoring system for new board members by pairing them with a more experienced 'buddy'. This system is aimed at providing guidance and support in the new role, and enabling the new board members to discuss and raise questions about how the board operates.
- **External relationships** – a number of positive comments were received on the Authority's relationships with both the sector and its users, commenting on the different methods of engagement such as the development of the new website and the clinic portal or the annual conference, and engaging with the key stakeholders in various HFEA campaigns and the Authority strategy.

3.9 The table below summaries the number of recommendations by rating and review area:

	Total Recs	High	Medium	Low
Board Effectiveness – self assessment	2	0	1	1

3.10 The two recommendations have been summarised below:

- **Sharing updates and news with the board members in between meetings could be extended:** The level of sharing information on the work of the Authority between board meetings and updates on implementation of agreed actions can be enhanced.

4. Further Training and development support for board members on corporate governance and their role: interviews with the board members indicate that additional training and development support on their role as a board member and the corporate governance framework would be welcome. Next Steps

4.1 To support the provision of a meaningful report to the Audit and Governance Committee you 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 form the basis of subsequent activity to verify that the recommendations have been implemented effectively. If management do not accept any of the recommendations made then a clear reason should be provided in the action plan.

4.3 Management should implement the agreed recommendations before or by the agreed due dates and advise HGIAS that the actions have been completed.

4.4 Any high priority recommendations are routinely followed up by HGIAS and any such outstanding actions will be reported to the Audit and Governance Committee.

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

5. Recommendations Table

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 actio n taken to implement the recommendation to take place.

№	RATING	RECOMMENDATIONS	MANAGEMENT RESPONSE	AGREED ACTION PLAN: OWNER & PLANNED IMPLEMENTATION DATE
1.	M	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.	Peter Thompson (Chief Executive) 30th May 2017
2.	L	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.	Peter Thompson (Chief Executive) 30th May 2017

6. Findings and Observations

6.1 Based on the survey and interviews, we have identified the following findings:

1. FINDING/OBSERVATION:

Information Sharing and Progress Updates

RISK RATING: MEDIUM

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.

RISK/IMPLICATION:

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.

RECOMMENDATION:

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.

2. FINDING/OBSERVATION:

Training and development support for board members on corporate governance and their role

RISK RATING: LOW

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.

RISK/IMPLICATION:

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.

RECOMMENDATION:

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.

Appendix 1 – Summary of Survey Results

1.1 Survey and interview results

Board Effectiveness Survey Category	Average survey score	Benchmark category
Purpose	5.58	Foundations
Composition and Structure	**5.38**	
Role Clarity	**5.42**	
Relationships	5.56	
Strategy	5.56	
Performance Monitoring	5.50	Board Focus
Risk & finance	5.57	
Decision making	5.50	
Stakeholder engagement	5.59	Engaging & Improving
Individual & whole Board	**5.33**	
Development & Succession Plans	**5.11**	
Chair	5.79	Chair
Total survey average	**5.50**	

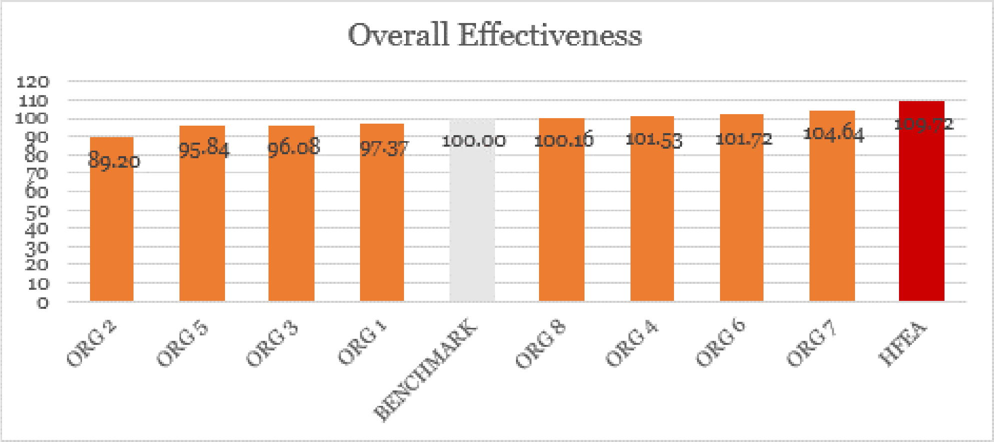
Survey scores used: 1 Strongly Disagree; 2 Disagree; 3 Slightly Disagree; 4 Slightly Agree; 5 Agree; 6 Strongly Agree

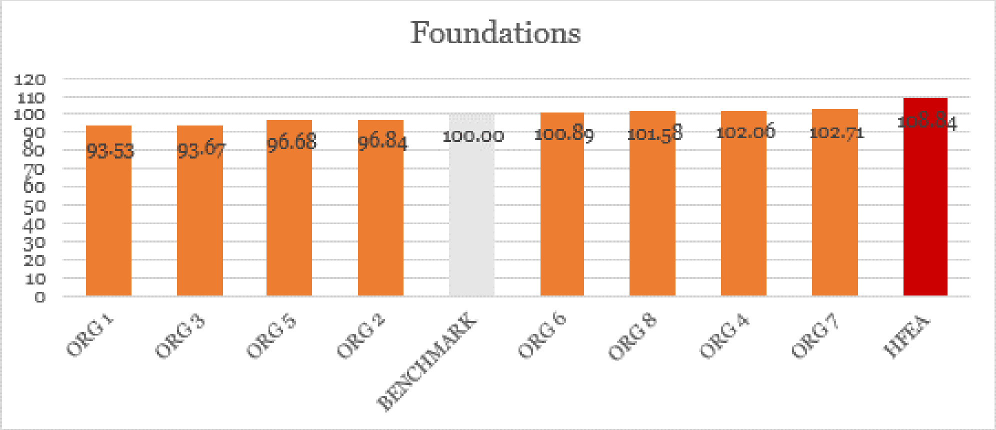
2.1 Benchmarking exercise

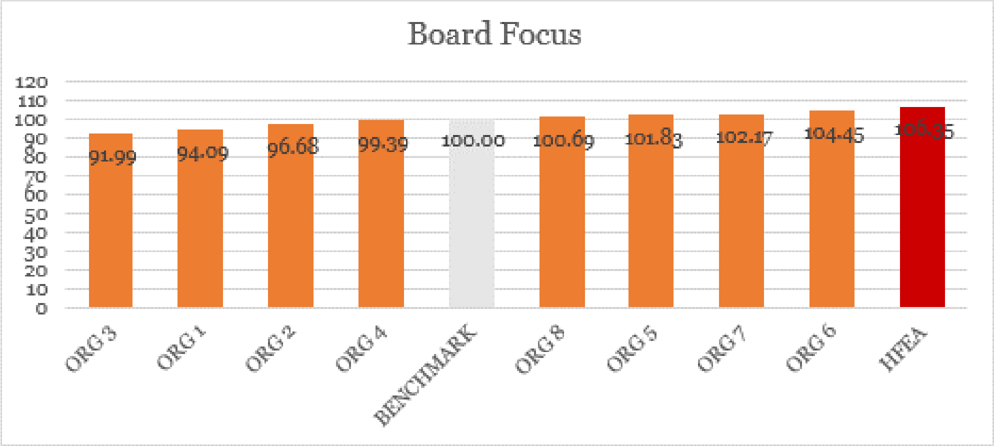
The benchmarking exercise shows the following results in the five categories:

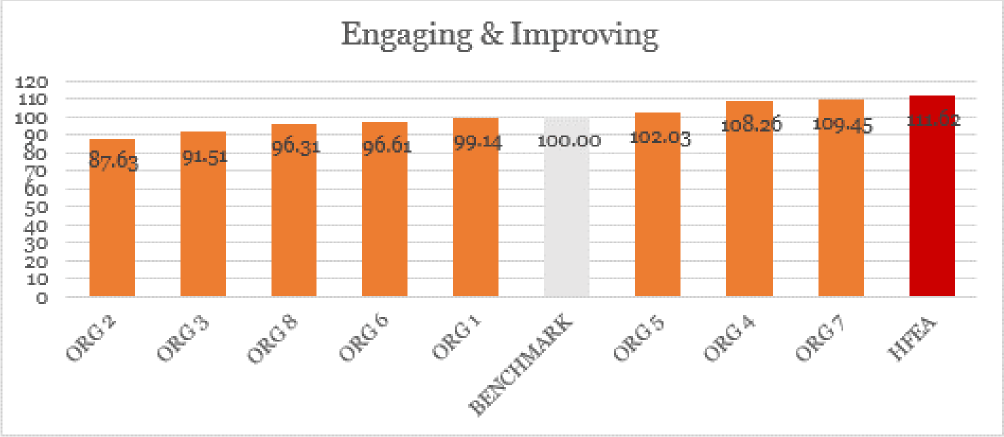
- Overall Effectiveness
- Foundations
- Board Effectiveness
- Engaging & Improving
- Chair

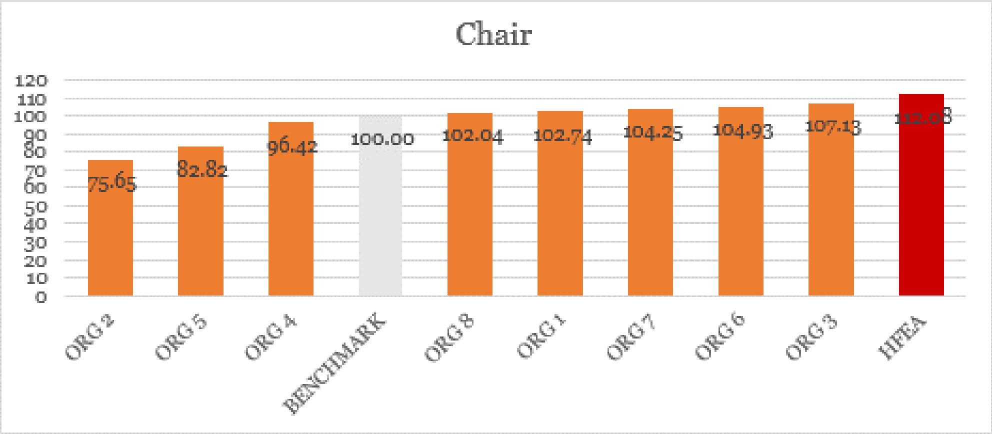
The benchmarking exercise was undertaken to compare HFEA's performance against other ALBs. While we are aware the other ALBs may have their boards structured differently from HFEA and roles may also differ (e.g. in reaching regulatory decisions), the focus of the survey was on the board members' views of the board effectiveness and therefore should represent a comparable view and benchmark for the organisation. The benchmark represents the average score of all responses denoted as 100 points, with organisations performing either above or below this benchmark indicated by their relative score.


Overall Effectiveness


Foundations


Board Focus


Engaging & Improving


Chair
120
110
100
90
80
70
60
50
40
30
20
10
0
75.65
82.82
96.42
100.00
102.04
102.74
104.25
104.93
107.13
112.08
ORG 2
ORG 5
ORG 4
BENCHMARK
ORG 8
ORG 1
ORG 7
ORG 6
ORG 3
HFEA

Appendix 2 – Risk and Report Ratings

Risk Ratings:

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

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.

Health Group Internal Audit

Reference: DHX216008003
FINAL REPORT
Human Fertilisation and
Embryology Authority
March 2017

Report Name: Information Standards

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.

Status: FINAL

For further information please contact:

Cameron Robson - 01132 54 5515

1N16 Quarry House, Quarry Hill, Leeds, LS2 7UE

Our work has been conducted and our report prepared solely for the benefit of the Department of Health and its arms length bodies and in accordance with a defined and agreed terms of reference. In doing so, we have not taken into account the considerations of any third parties. Accordingly, as our report may not consider issues relevant to such third parties, any use they may choose to make of our report is entirely at their own risk and we accept no responsibility whatsoever in relation to such use. Any third parties, requiring access to the report may be required to sign 'hold harmless' letters.

CONTENTS **PAGE**

1.	Introduction	1
2.	Review Conclusion	1
3.	Summary of Findings	2
4.	Next steps	2
5.	Recommendations	3
6.	Findings and Observations	4
	Appendix – Priority and Report Ratings	7

Date fieldwork completed:	25/01/2017
1st draft report issued:	10/02/2017
Management responses received:	03/03/2017
Final report issued	09/03/2017

Report Author: Nadene Coetzee
Version №: Final V1

Distribution List – Draft Report

Main recipient(s)

Juliet Tizzard	Director of Strategy and Corporate Affairs
Joanne Triggs	Head of Engagement

Cc(s)

Morounke Akingbola	Head of Finance
Richard Sydee	Director of Finance and Resources
Cameron Robson	Group Chief Head of Internal Audit

Distribution List – Final Report

As above

EXECUTIVE SUMMARY

1. Introduction

1.1 The HFEA is currently reviewing its document production processes, including working towards gaining the NHS England Information Standards accreditation for its patient facing information as a mark of quality.

1.2 The HFEA has recently submitted its application for the accreditation which details its systems and processes governing publication of information directed at patients. A further part of the accreditation process will involve both an inspection of its policies and some testing of staff awareness and compliance with the guidance.

1.3 As a result of the ongoing accreditation of patient facing information, it was agreed that within this review of HFEA's information production process, our focus would be limited to published corporate information on the HFEA's new website. This has avoided duplication with the NHS England work and allowed us to use the same principles from the Information Standard to create a framework against which we have assessed the policies and process for publication of corporate information.

1.4 The new HFEA website is currently live and accessible to the public, running alongside the old website until mid-March 2017. From that point, the old website will cease to be accessible.

2. Review Conclusion

2.1 The overall rating for the report is **Moderate** - some improvements are required to enhance the adequacy and effectiveness of the framework of producing corporate website content. The HFEA has been able to evidence progress made in embedding the corporate information standards set out in the "Producing corporate website content" document. Management is, though, still determining some parts of the process, for example whether to include a specific feedback button or not, and we have though identified some further actions that management could take to optimise the benefits of the corporate information standards.

3. Summary of Findings

3.1 The findings in this report are based on the available supporting evidence provided to us during our work. The review is intended to help the Head of Engagemnent enhance the effectiveness and implementation of the standards for corporate information by providing an independent and objective view of the progress in embedding the standards. The above conclusions and findings summarised below should be seen in this context.

3,2 The findings from our work are summarised below, and more detail is provided in the Findings and Observations section of this report (section 5):

- The workflows within the Content Management System (CMS) system are not currently configured to require approvals or enforce segregation of duties between writing, uploading and releasing publications to the new website.

- As 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, although this does appear to happen in practice. Consideration should be given to updating the guidance to require this step, possibly using a risk based approach depending on the content of the publication.

- We were unable to obtain written evidence of approval from the Head of Engagment and/or a Director for six of the eight publications selected for testing, although management confirmed that verbal approval had been provided.

3.3 There are still some parts of the process which management have yet to determine, in particular whether or not to include a specific 'Feedback' button to allow users to provide instant feedback if they notice information is incorrect or out of date. There is a 'Contact us' section which currently provides functionality to provide such feedback, although it may be more effective to utilise a dedicated 'Feedback' button. We have not raised this as a finding given it is already under consideration, but would encourage management to make a final decision and implement if appropriate.

3.4 Overall, management appears to be making good progress in implementing and embedding the Corporate information standards in relation to the publications made available on the website, but as identified above there is scope to formalise and evidence some elements of the process.

3.5 The table below summaries the number of recommendations by rating and review area:

Area	Total Recs	High	Medium	Low
Evidence sources	1	-	-	1
Review	1	-	-	1
End product	1	-	1	-
Total	**3**	**-**	**1**	**2**

4. Next Steps

4.1 To support continued progress with embedding the Corporate Information Standard's objectives into HFEA 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.

5. 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.	**M**	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. Owner: Jo Triggs (Head of Engagement)
2.	**L**	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. Owner: Jo Triggs (Head of Engagement) Date: 1 April
3.	**L**	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. Owner: Jo Triggs (Head of Engagement) Date: 1 April

6. Findings and Observations

1. FINDING/OBSERVATION:

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.

RISK RATING: MEDIUM

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.

RISK/IMPLICATION:

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.

RECOMMENDATION:

1. Until the issues within CMS are resolved, manual processes should be established to ensure that appropriate approval is obtained for all publications prior to release onto the website.
2. 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.

2. FINDING/OBSERVATION:

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

RISK RATING: LOW

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.

RISK/IMPLICATION:

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.

RECOMMENDATION:

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 should 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.

FINDINGS/OBSERVATIONS

3. FINDING/OBSERVATION:

Lack of written evidence of approval from the Head of Engagement and/or a Director for six of the eight publications selected for testing.

RISK RATING: LOW

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

RISK/IMPLICATION:

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.

RECOMMENDATION:

All approvals should be in writing to evidence that all publications have been appropriately reviewed and approved, and to provide a complete audit trail.

APPENDIX - PRIORITY AND REPORT RATING DEFINITIONS

Appendix – 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.

Human Fertilisation & Embryology Authority

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

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

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.

Our work has been conducted and our report prepared solely for the benefit of the Department of Health and its arms length bodies and in accordance with a defined and agreed terms of reference. In doing so, we have not taken into account the considerations of any third parties. Accordingly, as our report may not consider issues relevant to such third parties, any use they may choose to make of our report is entirely at their own risk and we accept no responsibility whatsoever in relation to such use. Any third parties, requiring access to the report may be required to sign 'hold harmless' letters.

CONTENTS **PAGE**

1. Introduction 1

2. Review Conclusion 1

3. Summary of Findings 2

4. Next steps 2

5. Recommendations 3

6. Findings and Observations 4

Appendix A – Priority and Report Ratings 5
Appendix B – Cloud 6

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

Health Group
Internal Audit

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.

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 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 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 <b>Password permission matrix</b> as well as a password policy within the Information Security Policies document.

Microsoft Azure have appropriate physical and logical security controls. They are <b>ISO27001</b> 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 <b>Government Cloud (G-Cloud)</b> 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 <b>Business Continuity</b> 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) :

<b>Standard tier</b>
<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 &lt; 12h, RPO &lt; 1h</td></tr>
<tr><td>Restore from Azure Backup Vault</td><td>ERT &lt; 12h, RPO &lt; 1 wk</td></tr>
<tr><td>Active Geo-Replication</td><td>ERT &lt; 30s, RPO &lt; 5s</td></tr>
</table>
<b>NOTE:</b> 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

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.

Resilience and Business continuity

Strategic delivery:	☒ Setting standards	☒ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item	9		
Paper number	AGC (21/03/2017) 536 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	As outlined		
Implementation date	Ongoing		
Communication(s)	Ongoing		
Organisational risk	☒ Low	☐ Medium	☐ High
Annexes			

1. Introduction

1.1. This brief paper outlines our arrangements for business continuity, for preparing and managing our activity in the event of loss of staff, information technology support, office accommodation.

1.2. The HFEA has Business Continuity Plan and a Pandemic Response Plan in place and named staff have responsibilities. Business continuity has a dedicated site in Office 365 where an up to date copy of the Business Continuity Plan and other key documents are made available. All HFEA staff have access to this facility, using their usual id and password, from any device, anywhere – and which also contains a newsfeed and a "Yammer" channel for communicating updates.

2. Effectiveness

2.1. We undertook a test of our emergency alert system, which sends text messages to all members of staff on 1 March 2017.

2.2. It is the case this met with limited success with just fewer than 50% responding to the message. We are currently reviewing the reasons for this limited engagement.

2.3. In any event, this indicates a need for reinforced awareness of business continuity arrangements for staff; the need for staff to advise the HFEA of changes in mobile phone number and a need for further training - all of which is being, or will be, addressed.

2.4. We are currently evaluating some new technology options with a view to being able to restore critical on premise systems on to a cloud environment in the event of Spring Gardens being unavailable for any length of time.

2.5. Since the last report to AGC there have been one significant BC related incident when power failed to Spring Gardens for three days – December 2016. The majority of staff were able to work from home as the move to Office 365 left email services unaffected.

2.6. It highlighted the need to migrate our records management system into the cloud. The BCP was updated with lessons learned from the outage.

3. Recommendation:

3.1. The Audit and Governance Committee is asked to:

- Note that business continuity arrangements are in place
- Note the poor response to the test emergency alert system.

4. Annexes:

- None

Human Fertilisation & Embryology Authority

Audit and Governance Committee Forward Plan

Strategic delivery:	☐ Setting standards	☐ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit & Governance Committee Forward Plan		
Agenda item	10		
Paper number	AGC (21/03/2017) 537		
Meeting date	21 March 2017		
Author	Morounke Akingbola, Head of Finance		
Output:			
For information or decision?	Decision		
Recommendation	The Committee is asked to review and make any further suggestions and comments and agree the plan.		
Resource implications	None		
Implementation date	N/A		
Organisational risk	☒ Low	☐ Medium	☐ High
	Not to have a plan risks incomplete assurance, inadequate coverage or unavailability key officers or information		
Annexes	N/A		

Audit & Governance Committee Forward Plan

AGC Items Date:	21 Mar 2017	13 Jun 2017	3 Oct 2017	5 Dec 2017
Following Authority Date:	10 May 2017	28 Jun 2017	15 Nov 2017	Jan 2018
Meeting 'Theme/s'	**Finance and Resources**	**Annual Reports, Information Governance, People**	**Strategy & Corporate Affairs, AGC review**	**Register and Compliance, Business Continuity**
Reporting Officers	**Director of Finance & Resources**	**Director of Finance & Resources**	**Director of Strategy & Corporate Affairs**	**Director of Compliance and Information**
Strategic Risk Register	Yes	Yes	Yes	Yes
Information for Quality (IfQ) Prog	Yes			Yes
Annual Report & Accounts (inc Annual Governance Statement)		Yes – For approval		
External audit (NAO) strategy & work	Interim Feedback	Audit Completion Report	Audit Planning Report	Audit Planning Report
Information Assurance & Security		Yes		
Internal Audit Recommendations Follow-up	Yes	Yes	Yes	Yes
Internal Audit	Results, annual opinion approve draft plan	Update	Update	Update
Whistle Blowing, fraud (report of any incidents)	Update as necessary	Update as necessary	Update as necessary	Update as necessary
Contracts & Procurement including SLA management	Update as necessary	Update as necessary	Update as necessary	Update as necessary

AGC Items Date:	21 Mar 2017	13 Jun 2017	3 Oct 2017	5 Dec 2017
HR, People Planning & Processes		Yes		
Strategy & Corporate Affairs management			Yes	
Regulatory & Register management				Yes
Resilience & Business Continuity Management				Yes
Finance and Resources management	Yes			
Reserves policy			Yes	
Review of AGC activities & effectiveness, terms of reference				Yes
Legal Risks	Yes			
AGC Forward Plan	Yes	Yes	Yes	Yes
Session for Members and auditors	Yes	Yes	Yes	Yes
Other one-off items				

Strategic risks

Strategic delivery:	☒ Setting standards	☒ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item	11		
Paper number	[AGC (21/03/2017) 537 PR]		
Meeting date	21 March 2017		
Author	Paula Robinson, Head of Business Planning		
Output:			
For information or decision?	Information and comment.		
Recommendation	AGC is asked to note the latest edition of the risk register, set out in the annex.		
Resource implications	In budget.		
Implementation date	Strategic risk register and operational risk monitoring: ongoing. CMG reviews risk quarterly in advance of each AGC meeting. AGC reviews the strategic risk register at every meeting. The Authority reviews the strategic risk register periodically.		
Organisational risk	☐ Low	☒ Medium	☐ High
Annexes	Annex 1: Strategic risk register		

1. Strategic risk register

Latest reviews

1.1. The Authority will receive the risk register at its meeting on 15 March. Any comments will be reported verbally at the meeting.

1.2. CMG reviewed the risk register at its meeting on 8 February. CMG reviewed all risks, controls and scores, and agreed to add a new risk relating to the forthcoming organisational changes that are being planned.

1.3. CMG also reviewed the two risks relating to donor conception and agreed to merge these into one single risk centred on running a good Opening the Register service.

1.4. CMG's comments are summarised on the second page of the risk register, which is attached at Annex A. The annex also includes the graphical overview of residual risks plotted against risk tolerances.

1.5. Four of the twelve risks are currently above tolerance.

1.6. This will be the last outing for the 2016/17 version of the strategic risk register. CMG will review the risk register afresh at its next meeting, to ensure alignment with the new strategy for 2017-2020, which will take effect in April.

2. Recommendation

2.1. AGC is asked to note the above, and to comment on the strategic risk register.

HFEA strategic risk register 2016/17

Risk summary: high to low residual risks

Risk area	Risk title	Strategic linkage[1]	Residual risk	Current status	Trend*
Information for Quality	IfQ1: Improved information access	Increasing and informing choice: information	**12 – High**	Above tolerance	⇔⇔⇩⇧
Information for Quality	IfQ3: Delivery of promised efficiencies	Efficiency, economy and value	**12 – High**	Above tolerance	⇔⇔⇧⇔
Data	D2: Incorrect data released	Efficiency, economy and value	**12 – High**	Above tolerance	⇔⇔⇧⇔
Capability	C1: Knowledge and capability	Efficiency, economy and value	**12 – High**	Above tolerance	⇔⇔⇧⇔
Legal challenge	LC1: Resource diversion	Efficiency, economy and value	**12 – High**	At tolerance	⇔⇔⇔⇔
Data	D1: Data loss or breach	Efficiency, economy and value	**10 – Medium**	At tolerance	⇔⇔⇔⇔
Organisational change	OC1: Change-related instability	Efficiency, economy and value	**9 – Medium**	At tolerance	• new
Financial viability	FV1: Financial resources	Efficiency, economy and value	**9 – Medium**	At tolerance	⇔⇔⇔⇔
Regulatory model	RM2: Loss of regulatory authority	Setting standards: quality and safety	**8 – Medium**	At tolerance	⇔⇔⇔⇔
Information for Quality	IfQ2: Register data	Increasing and informing choice: Register data	**8 – Medium**	At tolerance	⇔⇔⇔⇔
Regulatory model	RM1: Quality and safety of care	Setting standards: quality and safety	**4 – Low**	Below tolerance	⇔⇔⇔⇩
Opening the Register	OTR1: OTR service quality	Setting standards: donor conception	**4 – Low**	At tolerance	• new

* This column tracks the four most recent reviews by AGC, CMG, or the Authority (eg,⇧⇔⇩⇔).
Recent review points are: CMG 7 September/AGC 21 September ⇨ Authority 16 November ⇨ CMG 23 November/AGC 7 December ⇨ CMG 8 February

[1] Strategic objectives 2014-2017 (these will be updated in April when the new strategy has been launched):
Setting standards: improving the quality and safety of care through our regulatory activities. (Setting standards – quality and safety)
Setting standards: improving the lifelong experience for donors, donor-conceived people, patients using donor conception, and their wider families. (Setting standards – donor conception)
Increasing and informing choice: using the data in the register of treatments to improve outcomes and research. (Increasing and informing choice – Register data)
Increasing and informing choice: ensuring that patients have access to high quality meaningful information. (Increasing and informing choice – information)
Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government. (Efficiency, economy and value)

AGC – December 2016 meeting

The committee focused mainly on the three risks above tolerance at the time, which included Information for Quality (IfQ3) – delivery of promised efficiencies, Data (D2) – incorrect data release and Capability (C1) – knowledge and capability.

The committee questioned whether the Business Continuity Plan had been tested and was informed that there was an incident involving loss of power at the new HFEA premises in the summer of 2016 and the plan had been put into action. There were some lessons learned but generally things worked well.

The committee was concerned about the fluctuation of Parliamentary Questions that need to be answered within a tight timeframe and questioned how the organisation manages this area of work. The committee was informed that some questions could be tricky to answer. There is a small team of people in the organisation handling the questions, however the work is often extended to other staff with specialist knowledge to contribute to the answers. Answering parliamentary questions always takes priority in the organisation.

CMG – February 2017 meeting

CMG discussed in particular how best to reflect the risks associated with organisational change in the risk register. It was agreed that this should be presented as a separate, new, risk, in addition to the existing ‘business as usual’ risk relating to knowledge and capability.

We agreed that the financial viability risk should be updated, since year end and a new strategic period are approaching.

We also considered the two donor conception risks, and agreed that these should now be merged into one single risk centred on running a good Opening the Register service.

CMG updated all the remaining risks and controls and adjusted some of the residual risk scores to reflect the current situation.

We also noted that the risk register would need a comprehensive review as soon as the new strategy for 2017-2020 had been finalised, to ensure that it reflected the risks to delivering the strategy. It was agreed that the Chief Executive and the Head of Business Planning would work together to produce a draft, for comment at the next CMG risk meeting, in early May.

The Department of Health ALB risk network would be running a workshop on 28 February on risk interdependencies within the health system, between ALBs or with the Department itself. The HFEA would participate in this workshop, and the new version of the risk register would need to incorporate a section under each risk, identifying any interdependencies with other ALBs or the Department, within each risk. It had also been agreed that each ALB should prepare a report for its Audit Committee on risk interderdencies – this will be prepared for the next available AGC meeting after the notes of the workshop have been released (probably the June meeting, which would fit well with the Committee’s first review of the new version of the risk register to reflect the new strategy). Further reporting on health system risk interdependencies to DH or to auditors may be requested in the future, so it would be beneficial to have interdependencies identified separately and clearly in our risk register, along with any resulting controls or actions.

Criteria for inclusion of risks:

- Whether the risk results in a potentially serious impact on delivery of the HFEA's strategy or purpose.
- Whether it is possible for the HFEA to do anything to control the risk (so external risks such as weather events are not included).

Rank

The risk summary above is arranged in rank order according to the severity of the current residual risk score.

Risk trend

The risk trend shows whether the threat has increased or decreased recently. The direction of the arrow indicates whether the risk is: Stable ⇔ , Rising ⇧ or Reducing ⇩.

Risk scoring system

See last page.

Assessing inherent risk

Inherent risk is usually defined as 'the exposure arising from a specific risk before any action has been taken to manage it'. This can be taken to mean 'if no controls at all are in place'. However, in reality the very existence of an organisational infrastructure and associated general functions, systems and processes does introduce some element of control, even if no other mitigating action were ever taken, and even with no particular risks in mind. Therefore, in order for our estimation of inherent risk to be meaningful, the HFEA defines inherent risk as:

'the exposure arising from a specific risk before any additional action has been taken to manage it, over and above pre-existing ongoing organisational systems and processes.'

System-wide risk interdependencies

From April 2017 onwards, we will also explicitly consider whether any HFEA strategic risks or controls have a potential impact for, or interdependency with, the Department or any other ALBs. A distinct section to record any such interdependencies beneath each risk will be added to the risk register when it is reviewed to reflect the new strategy for 2017-2020, so as to be sure we identify and manage risk interdepencies in collaboration with relevant other bodies, and so that we can report easily and transparently on such interdependencies to DH or auditors as required.

<table>
<tr><th>Risk area</th><th>Description and impact</th><th>Strategic objective linkage</th><th colspan="3">Risk scores</th><th>Recent trend</th><th>Risk owner</th></tr>
<tr><td rowspan="7"><b>Regulatory model</b>
RM 1: Quality and safety of care</td><td rowspan="7">There is a risk of adverse effects on the quality and safety of care if the HFEA were to fail to deliver its duties under the HFE Act (1990) as amended.</td><td rowspan="7">Setting standards: improving the quality and safety of care through our regulatory activities.</td><td colspan="3">Inherent risk level:</td><td rowspan="7">⇔⇔⇔⇩</td><td rowspan="7">Peter Thompson</td></tr>
<tr><td>Likelihood</td><td>Impact</td><td>Inherent risk</td></tr>
<tr><td>3</td><td>5</td><td>15 High</td></tr>
<tr><td colspan="3"><b>Residual risk level:</b></td></tr>
<tr><td>Likelihood</td><td>Impact</td><td>Residual risk</td></tr>
<tr><td><b>1</b></td><td><b>4</b></td><td><b>4 Low</b></td></tr>
<tr><td colspan="2">Tolerance threshold:</td><td>8 Medium</td></tr>
</table>

Causes / sources	Mitigations	Timescale and ownership of mitigations	Commentary
Inspection/reporting failure.	Inspections are scheduled for the whole year, using licence information held on Epicentre, and items are also scheduled to committees well in advance.	In place – Sharon Fensome-Rimmer	Below tolerance. Some elements of this risk, associated with staff turnover and legal parenthood issues, have now reduced in likelihood, and so the residual risk level has reduced. On legal parenthood, a strong set of actions is in place and continues to be implemented. The inspection team continue to work with colleagues in licensed centres, with a focus on ensuring all affected patients are informed and appropriately supported.
	Audit of Epicentre conducted to reveal data errors in 2014/15. Error correction completed in 2016.	In place – Siobhain Kelly	
	Inspector training, competency-based recruitment, induction process, SOPs, QMS, and quality assurance all robust.	In place – Sharon Fensome-Rimmer	
Regulatory monitoring processes may be disrupted as a result of the temporary inability of Electronic Patient Record System (EPRS) providers to submit data to the new register structure until their software has been updated. This could impact performance information used in inspection notebooks and RBAT alerts.	Earlier agreements to extend IfQ delivery help to address this risk by extending the release date for the EDI replacement (IfQ release 2). Mitigation plans for this risk have been agreed as part of planning.	Mitigation in place - Nick Jones	
Monitoring failure.	Outstanding recommendations from inspection reports are tracked and followed up by the team.	In place – Sharon Fensome-Rimmer	
Unresponsiveness to or mishandling of non-compliances or grade A incidents.	Up to date compliance and enforcement policy.	In place – Nick Jones	
	Staffing model provides resilience in the inspection team for such events – dealing with high-impact cases, additional incident inspections, etc.	In place – Sharon Fensome-Rimmer	
Insufficient inspectors, administrative or licensing staff	Inspection team running at full complement.	In place – Nick Jones	
	Business support is operating below complement, and this will be addressed over the next few months, as part of organisational change implementation and the completion of IfQ.	To be addressed after IfQ, in the course of organisational restructuring – Sharon Fensome-Rimmer	

	Licensing team up to complement following earlier recruitment.	In place – Siobhain Kelly	
Recruitment difficulties and/or high turnover/churn in various areas; resource gaps and resource diversion into recruitment and induction, with impacts felt across all teams.	So far recruitment rounds have yielded sufficient candidates, although this has required going beyond the initial ALB pool to external recruitment in some cases.	Managed as needed – Sharon Fensome-Rimmer	
	Additional temporary resources available during periods of vacancy and transition.	In place – Rachel Hopkins	
	Group induction sessions put in place where possible.	In place – Sharon Fensome-Rimmer	
Resource strain itself can lead to increased turnover, exacerbating the resource strain.	Operational performance, risk and resourcing oversight through CMG, with deprioritisation or rescheduling of work an option.	In place – Paula Robinson	
Unexpected fluctuations in workload (arising from eg, very high level of PGD applications received, including complex applications involving multiple types of a condition; high levels of non-compliances either generally or in relation to a particular issue; introduction of mitochondrial treatment decision-making).	Staffing model amended in May 2015, to release an extra inspector post out of the previous establishment. This increased general resilience, enabling more flex when there is an especially high inspection/report writing/application processing workload.	In place – Sharon Fensome-Rimmer	
	Greater sector insight into our PGD application handling processes and decision-making steps achieved in the past few years; coupled with our increased processing rate since efficiency improvements were made in 2013 (acknowledged by the sector).	In place – Sharon Fensome-Rimmer	
Some unanticipated event occurs that has a big diversionary impact on key resources, eg, legal parenthood consent issues, or several major Grade A incidents occur at once.	Resilient staffing model in place.	In place – Sharon Fensome-Rimmer	
	Up to date compliance and enforcement policy and related procedures.	In place – Nick Jones / Sharon Fensome-Rimmer	
	A detailed action plan in response to the legal parenthood judgment is in place.	In progress – Nick Jones/Sharon Fensome-Rimmer	

<table>
<tr><th>Risk area</th><th>Description and impact</th><th>Strategic objective linkage</th><th colspan="3">Risk scores</th><th>Recent trend</th><th>Risk owner</th></tr>
<tr><td rowspan="7"><b>Regulatory model</b>
RM 2:
Loss of regulatory authority</td><td rowspan="7">There is a risk that the HFEA could lose authority as a regulator, jeopardising its regulatory effectiveness, owing to a loss of public / sector confidence.</td><td rowspan="7">Setting standards: improving the quality and safety of care through our regulatory activities.</td><td colspan="3">Inherent risk level:</td><td rowspan="7">⇔ ⇔ ⇔ ⇔</td><td rowspan="7">Peter Thompson</td></tr>
<tr><td>Likelihood</td><td>Impact</td><td>Inherent risk</td></tr>
<tr><td>3</td><td>5</td><td>15 High</td></tr>
<tr><td colspan="3"><b>Residual risk level:</b></td></tr>
<tr><td>Likelihood</td><td>Impact</td><td>Residual risk</td></tr>
<tr><td><b>2</b></td><td><b>4</b></td><td><b>8 Medium</b></td></tr>
<tr><td colspan="2">Tolerance threshold:</td><td>8 Medium</td></tr>
</table>

Causes / sources	Mitigations	Timescale and ownership of mitigations	Commentary
Failures or weaknesses in decision making processes.	Keeping up to date the standard operating procedures (SOPs) for licensing, representations and appeals.	In place – Siobhain Kelly	At tolerance. Although two additional risk sources exist at present (website outages until the new beta website is live and the plan of work to address legal parenthood consent issues), these are being well managed and/or tolerated, and the overall risk score has not increased.
	Learning from past representations and Appeal Committee hearings incorporated into processes.	In place – Siobhain Kelly	
	Appeals Committee membership maintained. Ongoing process in place for regular appointments whenever vacancies occur or terms of office end.	In place – Siobhain Kelly	
	Staffing structure for sufficient committee support.	In place – Siobhain Kelly	
	Decision trees; legal advisers familiar.	In place – Siobhain Kelly	
	Proactive management of quoracy for meetings.	In place – Siobhain Kelly	
	New (ie, first application) T&S licences delegated to ELP. Licensing Officer role in place to take certain administrative decisions from ELP.	In place – Siobhain Kelly	
Failing to demonstrate competence as a regulator	Up to date compliance and enforcement policy and related procedures.	In place – Nick Jones / Sharon Fensome-Rimmer	
	Inspector training, competency-based recruitment, induction process, SOPs, quality management system (QMS) and quality assurance all robust.	In place – Sharon Fensome-Rimmer	
Effect of publicised grade A incidents.	Staffing model provide resilience in inspection team for such events – dealing with high-impact cases, additional incident inspections, etc.	In place – Sharon Fensome-Rimmer	
	SOPs and protocols with Communications team.	In place – Sharon Fensome-Rimmer	
	Fairness and transparency in licensing committee information.	In place – Sharon Fensome-Rimmer	

	Dedicated section on website, so that the public can openly see our activities in the broader context.	In place – Sharon Fensome-Rimmer	
Administrative or information security failure, eg, document management, risk and incident management, data security.	Staff have annual information security training (and on induction).	In place – Dave Moysen	
	A comprehensive review of our records management practices and document management system (TRIM) will be conducted in 2017, following planned organisational changes and the conclusion of IfQ.	To follow – Peter Thompson	
	Guidance/induction in handling FOI requests, available to all staff.	In place – Siobhain Kelly	
	The IfQ website management project has reviewed the retention schedule.	Completed – August 2015 – Juliet Tizzard	
Until the IfQ website project has been completed, there is a continued risk of HFEA website outages, as well as difficulties in uploading updates to web pages.	Alternative mechanisms are in place for clinics to get information about materials such as the Code of Practice (eg, direct communications with inspectors, Clinic Focus).	In place – Sharon Fensome-Rimmer	
	The IfQ work on the new website will completely mitigate this risk (the new content management system will remove the current instability we are experiencing from using RedDot). This risk has informed our decisions about which content to move first to the beta version of the new site.	In progress – go live expected in March 2017 – Juliet Tizzard	
Negative media or criticism from the sector in connection with legally disputed issues or major adverse events at clinics.	HFEA approach is only to go into cases on the basis of clarifying legal principles or upholding the standards of care by challenging poor practice. This is more likely to be perceived as proportionate, rational and necessary (and impersonal), and is in keeping with our strategic vision.	In place - Peter Thompson	
HFEA process failings that create or contribute to legal challenges, or which weaken cases that are otherwise sound, or which generate additional regulatory sanctions activity (eg, legal parenthood consent).	Licensing SOPs, committee decision trees in place. Mitochondria donation application tools completed.	In place – Siobhain Kelly	
	Up to date compliance and enforcement policy and related procedures.	In place – Nick Jones / Sharon Fensome-Rimmer	
	Seeking the most robust possible assurance from the sector with respect to legal parenthood consent issues, and detailed plan in operation to address identified cases and anomalies.	In progress – Nick Jones	
	QMS and quality assurance in place in inspection team.	In place – Sharon Fensome-Rimmer	

Risk area	Description and impact	Strategic objective linkage	Risk scores			Recent trend	Risk owner
IfQ IfQ 1: Improved information access	If the information for Quality (IfQ) programme does not enable us to provide better information and data, and improved engagement channels, patients will not be able to access the improved information they need to assist them in making important choices.	Increasing and informing choice: ensuring that patients have access to high quality meaningful information.	Inherent risk level:			⇔ ⇔ ⇩ ⇧	Juliet Tizzard
			Likelihood	Impact	Inherent risk		
			4	4	16 High		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
			3	**4**	**12 High**		
			Tolerance threshold:		8 Medium		

Causes / sources	Mitigations	Timescale and ownership of mitigations	Commentary
Inability to extract reliable data from the Register.	Detailed planning and programme management in place to ensure this will be possible after migration. Migration strategy developed, and significant work being done to identify and cleanse all of the data that requires correction before migration. Decisions have been made about the degree of reliability required in each data field. For those fields where 100% reliability is needed, inaccurate or missing data is being addressed as part of project delivery.	All aspects – detailed project planning in place – Nick Jones	Above tolerance. It has been necessary to remain in beta for the website for far longer than originally planned, owing partly to a judicial review whose outcome is still awaited, and partly to protracted contractor resource negotiations and end-stage planning (now concluded, with final work in progress). Our final 'go live' GDS assessment for the website took place on 8 March. In the same time period, we are completing a detailed data verification process to update Choose a Fertility Clinic in readiness for Register migration and the new system, and this is proving challenging for the sector. Controls are in place, and it remains important for us
Reduced ability to provide for patient choice based on CaFC information as a result of EPRS inability to submit/correct data in the new register structure if they do not update their systems in time to comply. This could impact the publication of CaFC data.	Proposals on an updated IfQ delivery plan were agreed at August IfQ Programme Board, these should help address this risk. A mitigation and communication plan for this risk is in place, including ongoing dialogue with EPRS centres and providers.	In place - Nick Jones	
Stakeholders dislike or fail to accept the new model for CaFC. Stakeholders not on board with the changes.	In-depth stakeholder engagement and extensive user research completed to inform the programme's intended outcomes, products and benefits. This included, consultation, expert groups and Advisory Board and this continues to be an intrinsic part of programme approach.	In place and ongoing – Juliet Tizzard /Nick Jones	

Preparatory work to verify data in advance of the Register migration is effortful for clinics, with some struggling, and a risk that they could become disenchanted with IfQ or fail to see the future benefits.	Frequent sector communications about the current CaFC verification process, the reasons for it, and the ultimate pay-offs. Regular internal performance reports to track progress and problems. Focused support for the clinics who are struggling the most.	In place throughout the verification exercise – Nick Jones	to reiterate that the ultimate benefits of IfQ for the sector will make the extra effort invested now worthwhile.
Cost of delivering better information becomes too prohibitive, either because the work needed is larger than anticipated, or as a result of the approval periods associated with required DH/GDS gateway reviews (although these have improved markedly).	Costs were taken into account as an important factor in consideration of contract tenders and negotiations. Following earlier long timelines and unsuccessful attempts to discuss with GDS, our experience at the Beta gateway has been much improved and feedback was almost immediate. Watching brief being kept.	In place – Nick Jones In place – Nick Jones	
Redeveloped website does not meet the needs and expectations of our various user types.	Programme approach and some dedicated resources in place to manage the complexities of specifying web needs, clarifying design requirements and costs, managing changeable Government delegation and permissions structures, etc. User research done, to properly understand needs and reasons. Tendering and selection process included clear articulation of needs and expectations. GDS Beta assessment was passed on all 18 points.	In place – user research delivered end Oct 2016 – Juliet Tizzard	
Government and DH permissions structures are complex, lengthy, multi-stranded, and sometimes change mid-process.	Initial external business cases agreed and user research completed. Final business case for whole IfQ programme was submitted and eventually accepted. All GDS approvals sought so far have been granted, albeit with some delays to the earlier ones. Additional sprints of work were incorporated in beta, in an attempt to allow sufficient time (and resources) for the remaining GDS gateway review processes and subsequent formal approval mechanisms. The beta timeline was extended by 3 months to compensate for previous and anticipated future delays.	In place – Juliet Tizzard In place – Nick Jones (decision received April 2015) In place – Nick Jones	

Resource conflicts between delivery of website and business as usual (BAU).	Backfilling where possible/affordable to free up the necessary staff time, eg, Websites and Publishing Project Manager post backfilled to free up core staff for IfQ work.	In place – Juliet Tizzard	
Delivery quality is very supplier dependent. Contractor management has at times been very resource-intensive for staff. Work delivered by one or more suppliers could be poor quality and/or overrun, causing knock-on problems.	Programme management resources and quality assurance mechanisms in place for IfQ to manage (among other things) contractor delivery. Agile project approach includes a ‘one team’ ethos and requires close joint working and communication among all involved contractors. Sound project management practices in place to monitor delivery. Previous lessons learned and knowledge exist in the organisation from managing previous projects. Ability to consider deprioritising other work, through CMG, if necessary. Regular contract meetings in place.	In place – Juliet Tizzard	
New CMS (content management software) is ineffective or unreliable.	CMS options were scrutinised carefully as part of project. Appropriate new CMS chosen, and all involved teams happy with the selection.	In progress – implemented in beta phase, July 2016 – Juliet Tizzard	
Benefits not maximised and internalised into ways of working.	During IfQ delivery, product owners are in place, as is a communications plan. The aim is to ensure that changes are developed involving the right staff expertise (as well as contractors) and to ensure that the changes are culturally embraced and embedded into new ways of working. Knowledge handover with the contractors will take place.	In place – Nick Jones	

Annex A

Risk area	Description and impact	Strategic objective linkage	Risk scores			Recent trend	Risk owner
IfQ IfQ 2: Register data	HFEA Register data becomes lost, corrupted, or is otherwise adversely affected during IfQ programme delivery.	Increasing and informing choice: using the data in the Register of Treatments to improve outcomes and research.	Inherent risk level:			⇔ ⇔ ⇔ ⇔	Nick Jones
			Likelihood	Impact	Inherent risk		
			2	5	10 Medium		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
			2	**4**	**8 Medium**		
			Tolerance threshold:		8 Medium		

Causes / sources	Mitigations	Timescale and ownership of mitigations	Commentary
Risks associated with data migration to new structure, together with records accuracy and data integrity issues.	IfQ programme groundwork focused on current state of Register. Extensive planning in place, including detailed research and migration strategy.	In place – Nick Jones/Dave Moysen	At tolerance. This risk is being intensively managed – a major focus of IfQ planning work, particularly around data migration.
The firm (Avoca) which was scheduled to provide assurance on data migration has gone out of business.	The HFEA has considered other sources of assurance and sourced a supplier. Work is in progress.	In place – Nick Jones	
Historic data cleansing is needed prior to migration.	A detailed migration strategy is in place, and data cleansing is in progress.	In place – Nick Jones/Dave Moysen	
Increased reporting needs mean we later discover a barrier to achieving this, or that an unanticipated level of accuracy is required, with data or fields which we do not currently focus on or deem critical for accuracy.	IfQ planning work incorporated consideration of fields and reporting needs were agreed. Decisions about the required data quality for each field were ‘future proofed’ as much as possible through engagement with stakeholders to anticipate future needs and build these into the design.	In place – Nick Jones	
Reliability of existing infrastructure systems – (eg, Register, EDI, network, backups).	Maintenance of desktop, network, backups, etc. core part of IT business as usual delivery.	In place – Dave Moysen	
System interdependencies change / are not recognised	Strong interdependency mapping done between IfQ and business as usual.	Done – Nick Jones	
Benefits not maximised and internalised into ways of working.	During IfQ delivery, product owners are in place, as is a communications plan. The aim is to ensure that changes are developed involving the right staff expertise (as well as contractors) and to ensure that the changes are culturally embraced and embedding into new ways of working. Knowledge handover with the contractors will take place.	In place – Nick Jones	

<table>
<tr><th>Risk area</th><th>Description and impact</th><th>Strategic objective linkage</th><th colspan="3">Risk scores</th><th>Recent trend</th><th>Risk owner</th></tr>
<tr><td rowspan="7"><b>IfQ</b>

IfQ 3:
Delivery of promised efficiencies</td><td rowspan="7">There is a risk that the HFEA's promises of efficiency improvements in Register data collection and submission are not ultimately delivered.</td><td rowspan="7">Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government.</td><td colspan="3">Inherent risk level:</td><td rowspan="7">⇔⇔⇧⇔</td><td rowspan="7">Nick Jones</td></tr>
<tr><td>Likelihood</td><td>Impact</td><td>Inherent risk</td></tr>
<tr><td>4</td><td>4</td><td>16 High</td></tr>
<tr><td colspan="3"><b>Residual risk level:</b></td></tr>
<tr><td>Likelihood</td><td>Impact</td><td>Residual risk</td></tr>
<tr><td><b>3</b></td><td><b>4</b></td><td><b>12 High</b></td></tr>
<tr><td colspan="2">Tolerance threshold:</td><td>9 Medium</td></tr>
</table>

Causes / sources	Mitigations	Timescale and ownership of mitigations	Commentary
Poor user acceptance of changes, or expectations not managed.	Stakeholder involvement strategy in place and user testing being incorporated into implementation phases of projects.	In place – Nick Jones/Juliet Tizzard	Above tolerance. In November 2016, in light of delays to release two of the portal (which includes the new electronic data interchange system for data submission by clinics), we increased the risk level. The delays stem from the intensive work in progress to complete release one of the website, which requires the attention of the same staff who are needed for release two of the portal.
Clinics not consulted/involved enough.	Working with stakeholders has been central to the development of IfQ, and will continue to be. Advisory Group and expert groups have ended, but a stakeholder group for the implementation phase is in place. Workshops were delivered with the sector regarding how information will be collected through the clinic portal. From beta live onwards we will receive feedback and iteratively develop the products.	In place – Nick Jones/Juliet Tizzard	
Scoping and specification are insufficient for realistic resourcing and on-time delivery of changes.	Scoping and specification were elaborated with stakeholder input, so as to inform the tender. Resourcing and timely delivery were a critical part of the decision in awarding the contract.	In place and contracts awarded (July 2015) – Nick Jones	
Efficiencies cannot, in the end, be delivered.	Detailed scoping phase included stakeholder input to identify clinic users' needs accurately. Specific focus in IfQ projects on efficiencies in data collected, submission and verification, etc.	In place – Nick Jones	
Cost of improvements becomes too prohibitive, or resources are insufficient to complete the Programme.	Contracts only awarded to bidders who made an affordable proposal. Detailed planning for release two (which includes the second iteration of the portal and the introduction of the new EDI interface) is in progress and the HFEA will continue to work within agreed costs.	In place (July 2015) – Nick Jones In progress (September 2016 to present) – Nick Jones	

	A contingency amount was built into the budget, although this has now been used. The support function has been re-shaped and streamlined to deal with the departure in November 2016 of the release two project manager.	In place (from November 2016) – Nick Jones
Delivery is delayed, causing reputational damage to the HFEA.	Ongoing communication with clinics via Clinic Focus and direct correspondence, to keep them up to date and make them aware of delays.	In place – Nick Jones
Required GDS gateway approvals are delayed or approval is not given.	All GDS approvals sought so far have been granted, albeit with some delays to earlier gateways. Our detailed planning includes addressing the requirements laid down by GDS as conditions of alpha and beta phase approval. Additional sprints of work were incorporated into beta, in an attempt to allow sufficient time (and resources) for the remaining GDS gateway review processes and subsequent formal approval mechanisms. The beta timeline was extended by 3 months to compensate for previous and anticipated future delays.	In place – Nick Jones
Benefits not maximised and internalised into ways of working.	During IfQ delivery, product owners are in place, as is a communications plan. The aim is to ensure that changes are developed involving the right staff expertise (as well as contractors) and to ensure that the changes are culturally embraced and embedded into new ways of working. Knowledge handover with the contractors will take place.	In place (from June 2015) – Nick Jones
Planned organisational changes to ensure the HFEA can make full use of the new functionality delivered through IfQ could create risks to the completion of IfQ (release 2).	Staff consultation in progress. Additional resources within IfQ to ensure that delivery continues. In the event of turnover or other disruption to IfQ arising from organisational change, we will continue as now to seek temporary cover for vacancies.	In place – Nick Jones

Risk area	Description and impact	Strategic objective linkage	Risk scores			Recent trend	Risk owner
Legal challenge LC 1: Resource diversion	There is a risk that the HFEA is legally challenged in such a way that resources are significantly diverted from strategic delivery.	Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government.	Inherent risk level:			⇔ ⇔ ⇔ ⇔	Peter Thompson
			Likelihood	Impact	Inherent risk		
			5	4	20 Very high		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
			4	**3**	**12 High**		
			Tolerance threshold:		12 High		

Causes / sources	Mitigations	Timescale and ownership of mitigations	Commentary
Complex and controversial area.	Panel of legal advisors from various firms at our disposal for advice, as well as in-house Head of Legal.	In place – Peter Thompson	At tolerance. **Current cases:** The judgment in 2015 and subsequent cases on consents for parenthood have administrative and policy consequences for the HFEA. Further cases are going through court. The HFEA is unlikely to participate in most of these legal proceedings directly, though the court has required us to provide information and clarification in relation to six legal parenthood cases. The hearing for these six cases is listed for May 2017. A judicial review hearing of one discrete element of the IfQ CaFC project was held in December 2016 and January 2017. The outcome may impact on the presentation of our data in the new version of choose a fertility clinic.
	Evidence-based policy decision-making and horizon scanning for new techniques.	In place – Joanne Anton	
	Robust and transparent processes in place for seeking expert opinion – eg, external expert advisers, transparent process for gathering evidence, meetings minuted, papers available online.	In place – Joanne Anton/Juliet Tizzard	
HFE Act and regulations lead to the possibility of there being differing legal opinions from different legal advisers, that then have to be decided by a court.	Panel in place, as above, to get the best possible advice. Case by case decisions regarding what to argue in court cases, so as to clarify the position.	In place – Peter Thompson	
Decisions and actions of the HFEA and its committees may be contested. New guide to licensing and inspection rating (effective from go-live of new website) on CaFC may mean that more clinics make representations against licensing decisions.	Panel in place, as above.	In place – Peter Thompson	
	Maintaining, keeping up to date and publishing licensing SOPs, committee decision trees etc. consistent decision making at licence committees supported by effective tools for committees Standard licensing pack completely refreshed and distributed to members/advisers (April 2015).	In place – Siobhain Kelly	
	Well-evidenced recommendations in inspection reports.	In place – Sharon Fensome-Rimmer	
Subjectivity of judgments means the HFEA often cannot know in advance which way a ruling will go, and the extent to which costs and other resource demands may result from a case.	Scenario planning is undertaken at the initiation of any likely action.	In place – Peter Thompson	

HFEA could face unexpected high legal costs or damages which it could not fund.	If this risk was to become an issue then discussion with the Department of Health would need to take place regarding possible cover for any extraordinary costs, since it is not possible for the HFEA to insure itself against such an eventuality, and not reasonable for the HFEA's small budget to include a large legal contingency. This is therefore an accepted, rather than mitigated risk. It is also interdependent risk because DH would be involved in resolving it.	In place – Peter Thompson	
Legal proceedings can be lengthy and resource draining.	Panel in place, as above, enabling us to outsource some elements of the work.	In place – Peter Thompson	
	Internal mechanisms (such as the Corporate Management Group, CMG) in place to reprioritise work should this become necessary.	In place – Peter Thompson	
Adverse judgments requiring us to alter or intensify our processes, sometimes more than once.	Licensing SOPs, committee decision trees in place.	In place – Siobhain Kelly	

Risk area	Description and impact	Strategic objective linkage	Risk scores	Recent trend	Risk owner
Data D 1: Data loss or breach	There is a risk that HFEA data is lost, becomes inaccessible, is inadvertently released or is inappropriately accessed.	Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government.	Inherent risk level: Likelihood | Impact | Inherent risk 4 | 5 | 20 Very high Residual risk level: Likelihood | Impact | Residual risk **2** | **5** | **10 Medium** Tolerance threshold: 10 Medium	⇔⇔⇔⇔	Nick Jones

Causes / sources	Mitigations	Timescale and ownership of mitigations	Commentary
Confidentiality breach of Register data.	Staff have annual compulsory security training to guard against accidental loss of data or breaches of confidentiality. Secure working arrangements for Register team, including when working at home.	In place – Dave Moysen	At tolerance.
Loss of Register or other data.	As above.	In place – Dave Moysen	
	Robust information security arrangements, in line with the Information Governance Toolkit, including a security policy for staff, secure and confidential storage of and limited access to Register information, and stringent data encryption standards.	In place – Dave Moysen	
Cyber-attack and similar external risks.	Secure system in place as above, with regular penetration testing.	In place – Dave Moysen	
Infrastructure turns out to be insecure, or we lose connection and cannot access our data.	IT strategy agreed, including a thorough investigation of the Cloud option, security, and reliability.	In place – Dave Moysen	
	Deliberate internal damage to infrastructure, or data, is controlled through off-site back-ups and the fact that any malicious tampering would be a criminal act.	In place (March 2015) – Nick Jones	
Business continuity issue.	BCP in place and staff communication procedure tested. A new BCP is being produced by the Head of IT to reflect the changes to this following changes to infrastructure and the office move.	In place – Richard Sydee Update done Dave Moysen – September 2016	
Register data becomes corrupted or lost somehow.	Back-ups and warehouse in place to ensure data cannot be lost.	In place – Nick Jones/Dave Moysen	

Other HFEA data (system or paper) is lost or corrupted.	As above. Staff have annual compulsory security training to guard against accidental loss of data or breaches of confidentiality.	In place – Dave Moysen	
Poor records management	A comprehensive review of our records management practices and document management system (TRIM) will be conducted in 2017, following planned organisational changes and the conclusion of IfQ.	To follow – Peter Thompson	

<table>
<tr><th>Risk area</th><th>Description and impact</th><th>Strategic objective linkage</th><th colspan="3">Risk scores</th><th>Recent trend</th><th>Risk owner</th></tr>
<tr><td rowspan="7"><b>Data</b>
D 2:
Incorrect data released</td><td rowspan="7">There is a risk that incorrect data is released in response to a Parliamentary question (PQ), or a Freedom of Information (FOI) or data protection request.</td><td rowspan="7">Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government.</td><td colspan="3">Inherent risk level:</td><td rowspan="7">⇔⇔⇧⇔</td><td rowspan="7">Juliet Tizzard</td></tr>
<tr><td>Likelihood</td><td>Impact</td><td>Inherent risk</td></tr>
<tr><td>5</td><td>4</td><td>20 Very high</td></tr>
<tr><td colspan="3">Residual risk level:</td></tr>
<tr><td>Likelihood</td><td>Impact</td><td>Residual risk</td></tr>
<tr><td><b>3</b></td><td><b>4</b></td><td><b>12 High</b></td></tr>
<tr><td colspan="2">Tolerance threshold:</td><td>8 Medium</td></tr>
</table>

Causes / sources	Mitigations	Timescale and ownership of mitigations	Commentary
Poor record keeping	A comprehensive review of our records management practices and document management system (TRIM) will be conducted in 2017, following planned organisational changes and the conclusion of IfQ.	To follow – Peter Thompson	Above tolerance. Although we have some good controls in place for dealing with PQs and other externally generated requests, it should be noted that we cannot control incoming volumes, complexity or deadlines.
	Audit of Epicentre completed in 2014/15, errors corrected in 2016.	In place – Siobhain Kelly	
Excessive demand on systems and over-reliance on a few key expert individuals – request overload – leading to errors	PQs, FOIs and OTRs have dedicated expert staff/teams to deal with them. If more time is needed for a complex PQ, it is occasionally necessary to take the issue out of the very tightly timed PQ process and replace this with a more detailed and considered letter back to the enquirer so as to provide the necessary level of detail and accuracy in the answer. We also refer back to previous answers so as to give a check, and to ensure consistent presentation of similar data. FOI requests are refused when there are grounds for this.	In place – Juliet Tizzard / Nick Jones	
	PQ SOP revised and log created, to be maintained by Committee and Information Officer/Scientific Policy Manager.	In place - Siobhain Kelly	

Staff turnover resulting in the loss of corporate knowledge regarding the history and handling of PQs, in particular, resulting in slower handling and therefore potential reputational effect with the Department of Health.	Staff have access to past records to inform new responses. Recruitment completed in January 2017. Additional legal advice will be sought when beneficial. Good lines of communication with the Department so that any difficulties can be highlighted at the earliest possible point.	In place – Siobhain Kelly	
Answers in Hansard may not always reflect advice from HFEA.	The PQ team attempts to catch any changes to drafted wording that may unwittingly have changed the meaning. HFEA's suggested answer and DH's final submission both to be captured in new PQ log.	In place – Siobhain Kelly / Peter Thompson	
Insufficient understanding of underlying system abilities and limitations, and/or of the topic or question, leading to data being misinterpreted or wrong data being elicited.	As above – expert staff with the appropriate knowledge and understanding in place.	In place – Juliet Tizzard / Nick Jones	

Risk area	Description and impact	Strategic objective linkage	Risk scores			Recent trend	Risk owner
Opening the Register OTR 1: OTR service quality	There is a risk that OTR service quality is adversely affected by data accuracy, inadequate support, or human error.	Setting standards: improving the lifelong experience for donors, donor-conceived people, patients using donor conception, and their wider families.	Inherent risk level:			● New (combined from two previous risks)	Nick Jones
			Likelihood	Impact	Inherent risk		
			3	5	15 High		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
			1	**4**	**4 Low**		
			Tolerance threshold:		4 Low		

Causes / sources	Mitigations	Timescale and ownership of mitigations	Commentary
Data accuracy in Register submissions.	Continuous work with clinics on data quality, including current verification processes, steps in the OTR process, regular audit alongside inspections, and continued emphasis on the importance of life-long support for donors, donor-conceived people and parents.	In place – Nick Jones	At tolerance (which is low for this risk). The pilot counselling service has been in place since 1 June 2015, with annual assessment reports to Authority.
	Audit programme to check information provision and accuracy.	In place – Nick Jones	
	IfQ work has identified data accuracy requirements for different fields as part of migration planning, and will put in place more efficient processes.	In place – Nick Jones	
	If subsequent work or data submissions reveal an unpreventable earlier inaccuracy (or an error), we explain this transparently to the recipient of the information, so it is clear to them what the position is and why this differs from the earlier provided data.	In place – Nick Jones	
	Data verification work (February 2017) in preparation for Register migration will improve overall data accuracy, and the exercise includes tailored support for individual clinics that are struggling.	In place – Nick Jones	
Lack of counselling availability for applicants.	Counselling service established with external contractor in place.	In place (June 2015 onwards) – Nick Jones	

Insufficient Register team resource to deal properly with OTR enquiries and associated conversations.	Additional member of staff dedicated to handling such enquiries. IfQ delivery means there is still pressure on team capacity, and there has been a long term vacancy in the team, but this post has now been filled (start date 20 February 2017).	In place, with team capacity issue close to resolution (February 2017) – Nick Jones
Risk of inadequate handling of a request.	Trained staff, SOPs and quality assurance in place.	In place – Nick Jones
	SOPs reviewed by Register staff, CMG and PAC-UK, as part of the pilot set-up. Contract in place with PAC-UK for pilot delivery.	Done (May 2015) – ongoing management of the pilot by Rosetta Wotton.
Issuing of wrong person's data.	OTR process has an SOP that includes specific steps to check the information given and that it relates to the right person.	In place – Nick Jones
Process error or human error.	As above.	In place – Nick Jones

Risk area	Description and impact	Strategic objective linkage	Risk scores			Recent trend	Risk owner
Financial viability FV 1: Income and expenditure	There is a risk that the HFEA has insufficient financial resources to fund its regulatory activity and strategic aims.	Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government.	Inherent risk level:			⇔⇔⇔⇔	Richard Sydee
			Likelihood	Impact	Inherent risk		
			4	4	16 High		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
			3	**3**	**9 Medium**		
			Tolerance threshold:		9 Medium		

Causes / sources	Mitigations	Timescale and ownership of mitigations	Commentary
The complexity of accurately forecasting income, which is linked directly to treatment activity in licensed establishments, exposes HFEA to significant variability in annual income.	Activity levels are tracked and change is discussed at CMG, who would consider what work to deprioritise and reduce expenditure.	Monthly (on-going) – Richard Sydee	At tolerance. At M10 (January) we have a surplus of £642k before IfQ. The increase in fees approved by Treasury in 2015/16 continues to impact on the surplus being reported and we expect this to continue into the new business year. We will continue to monitor activity levels monthly. The creation of the Intelligence team post IfQ implementation allows for more detailed analysis and potentially forecasting of activity levels.
	Fees Group created enabling dialogue with sector about fee levels. Fee increase was agreed and approved by Treasury. This was implemented and the eSET discount ended (April 2016).	In place. Fees Group ongoing – Richard Sydee	
	Worked planned in 2017/18 to better understand the likely future trends in treatment cycle activity.	Being planned – Richard Sydee	
GIA funding could be reduced due to changes in Government/policy.	A good relationship with DH Sponsors, who are well informed about our work and our funding model.	Accountability Quarterly meetings (on-going) – Richard Sydee	
	Annual budget agreed with DH Finance team alongside draft business plan submission. GIA funding has been provisionally agreed through to 2020.	December annually – Richard Sydee	
	Detailed budgets for 2017/18 have been agreed with Directors. DH has previously agreed our resource envelope.	In place – Morounke Akingbola	
Annual budget setting process lacks information from directorates on variable/additional activity that will impact on planned spend.	Annual budgets are agreed in detail between Finance and Directorates with all planning assumptions noted. Quarterly meetings with directorates flags any shortfall or further funding requirements.	Quarterly meetings (on-going) – Morounke Akingbola	
Legal costs materially exceed annual budget as a result of unforeseen litigation.	Use of reserves, up to contingency level available. DH kept abreast of current situation and are a final source of additional funding if required.	Monthly – Morounke Akingbola	

Upwards scope creep during projects, or emerging during early development of projects.	Senior Finance staff present at Programme Board. Periodic review of actual and budgeted spend by IfQ project board and monthly budget meetings with finance.	Ongoing – Richard Sydee or Morounke Akingbola	
	Cash flow forecast updated.	Monthly (on-going) – Morounke Akingbola	

<table>
<tr><th>Risk area</th><th>Description and impact</th><th>Strategic objective linkage</th><th colspan="3">Risk scores</th><th>Recent trend</th><th>Risk owner</th></tr>
<tr><td rowspan="7"><b>Capability</b>
C 1: Knowledge and capability</td><td rowspan="7">There is a risk that the HFEA experiences unforeseen knowledge and capability gaps, threatening delivery of the strategy.</td><td rowspan="7">Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government.</td><td colspan="3">Inherent risk level:</td><td rowspan="7">⇔ ⇔ ⇧ ⇔</td><td rowspan="7">Peter Thompson</td></tr>
<tr><td>Likelihood</td><td>Impact</td><td>Inherent risk</td></tr>
<tr><td>4</td><td>4</td><td>16 High</td></tr>
<tr><td colspan="3">Residual risk level:</td></tr>
<tr><td>Likelihood</td><td>Impact</td><td>Residual risk</td></tr>
<tr><td><b>4</b></td><td><b>3</b></td><td><b>12 High</b></td></tr>
<tr><td colspan="2">Tolerance threshold:</td><td>6 Medium</td></tr>
</table>

Causes / sources	Mitigations	Timescale and ownership of mitigations	Commentary
Organisational change	See separate risk, below.		
High turnover, sick leave etc. leading to temporary knowledge loss and capability gaps.	People strategy will partially mitigate. Mixed approach of retention, staff development, and effective management of vacancies and recruitment processes.	Done – May 2015 – Rachel Hopkins	Above tolerance. This risk and the set of controls remains focused on business as usual capability, rather than capacity. There are obviously some linkages between capability and capacity, since managing turnover and churn also means managing fluctuations in capability and ensuring knowledge and skills are successfully nurtured and/or handed over. Organisational change is also a factor that can affect this general risk – this has been identified as a separate strategic risk (see below). Since the HFEA is a small organisation, with little intrinsic resilience, it seems prudent to retain a low tolerance level for this risk. Several staff (including end of contract IfQ staff) have left the organisation in the past six months. This means we are currently in a period of turnover
	Staff have access to civil service learning (CSL); organisational standard is five working days per year of learning and development for each member of staff.	In place – Rachel Hopkins	
	Organisational knowledge captured via records management (TRIM), case manager software, project records, handovers and induction notes, and manager engagement.	In place – Rachel Hopkins	
	Vacancies are addressed speedily, and any needed changes to ways of working or backfill arrangements receive immediate attention.	In place – Peter Thompson	
	Staff are encouraged to identify personal development opportunities with their manager, through the PDP process, making good use of CSL.	In place – Peter Thompson	
The government may implement further cuts across all ALBs, resulting in further staffing reductions. This would lead to the HFEA having to reduce its workload in some way.	The HFEA was proactive in reducing its headcount and other costs to minimal levels over a number of years. We have also been reviewed extensively (including the McCracken review, and our recent Triennial Review). Turnover is variable, and so this risk will be retained on the risk register, and will continue to receive ongoing management attention.	In place – Peter Thompson	

Poor morale leading to decreased effectiveness and performance failures.	Engagement with the issue by managers. Ensuring managers have team meetings and one-to-one meetings to obtain feedback and identify actions to be taken.	In place – Peter Thompson	and internal churn, with some knowledge gaps, and IfQ work ongoing for both release one (although this is now close to completion) and release two.
	Staff survey and implementation of outcomes, followed up after December 2016 all staff conference. Task and Finish Groups working on recommendations for improvements.	Survey and staff conference done – Rachel Hopkins Follow-up plan and communications in place – Peter Thompson	
Particular changes or other pressures for individual teams could lead to specific areas of knowledge loss and low performance.	CMG and managers prioritise work appropriately when workload peaks arise.	In place – Peter Thompson	
	Policies and processes to treat staff fairly and consistently, particularly in scenarios where people are or could be 'at risk'.	In place – Peter Thompson	
Additional avenues of work open up, or reactive diversions arise, and need to be accommodated alongside business as usual and (at present) the major IfQ programme.	Careful planning and prioritisation of both business plan work and business flow through our Committees. Regular oversight by CMG – standing item on planning and resources.	In place – Paula Robinson	
	Early emphasis given to team-level service delivery planning in preparation for the next business year, with active involvement of team members. CMG will continue to review planning and delivery.	In place – Paula Robinson	
	Planning prioritises IfQ delivery, and therefore strategy delivery, within our limited resources.	In place as part of business planning until IfQ ends (2015 to 2017) – Paula Robinson	
	IfQ has some of its own dedicated resources.	In place – Nick Jones	
	There is a degree of flexibility within our resources, and increasing resilience is a key consideration whenever a post becomes vacant.	In place – Peter Thompson	
Regarding the recent work on licensing mitochondrial replacement techniques, there is a possible future risk that we will need to increase both capability and capacity in this area, depending on uptake (this is not yet certain).	Future needs (capability and capacity) relating to mitochondrial replacement techniques and licensing applications are starting to be considered now, but will not be known for sure until later. No controls can yet be put in place, but the potential issue is on our radar, since it could impact on staff and committee capacity. For now it seems clear that only one clinic will be making applications and that there will not be large numbers of these. New licensing processes are in place, ready for first use (decision trees etc.).	Issue for further consideration when applications begin to be considered – Juliet Tizzard	

Our IT communications systems are an inherent part of our general capability, and since our office move in 2016, we have experienced some technical infrastructure issues with Skype. This leads to poor service (missed calls, poor quality Skype meetings), reputational impacts, additional costs (meetings having to be held externally using non-Skype videoconferencing equipment), and potentially to complaints. Staff are incurring additional work and additional travel, to find and test their own work-arounds so as to avoid using Skype for decision-making meetings until the problems are fixed. This is compounded by a shortage of non-Skype-based videoconferencing solutions in conference venues.	IT team working to identify and resolve the issues, with staff encouraged to continue to send support tickets. External expert commissioned to assist. Staff running meetings continue to source external venues with appropriate facilities so as to avoid reliance on our own equipment until the problems have been solved. Use of mailboxes to provide an alternative channel when Skype calls are not received (however there are also some problems with these too).	In progress – Dave Moysen and Nick Jones	

<table>
<tr><th>Risk area</th><th>Description and impact</th><th>Strategic objective linkage</th><th colspan="3">Risk scores</th><th>Recent trend</th><th>Risk owner</th></tr>
<tr><td rowspan="7"><b>Organisa-tional change</b>

OC1: Change-related instability</td><td rowspan="7">There is a risk that the implementation of organisational changes is poor, resulting in instability, loss of capability and capacity, and delays in the delivery of the strategy.</td><td rowspan="7">Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government.</td><td colspan="3">Inherent risk level:</td><td rowspan="7">● New</td><td rowspan="7">Peter Thompson</td></tr>
<tr><td>Likelihood</td><td>Impact</td><td>Inherent risk</td></tr>
<tr><td>4</td><td>4</td><td>16 High</td></tr>
<tr><td colspan="3">Residual risk level:</td></tr>
<tr><td>Likelihood</td><td>Impact</td><td>Residual risk</td></tr>
<tr><td><b>3</b></td><td><b>3</b></td><td><b>9 Medium</b></td></tr>
<tr><td colspan="2">Tolerance threshold:</td><td>9 Medium</td></tr>
</table>

Causes / sources	Mitigations	Timescale and ownership of mitigations	Commentary
Until the new model is formally decided, there will be a level of uncertainty among staff about their own or their colleagues' future roles. This initial phase and then the change period itself may lead to dips in morale, commitment, discretionary effort and goodwill. Anxieties about change during the whole process may sometimes lead to stress behaviours which decrease performance and damage delivery. It is possible that we could reach a tipping point where staff are less productive, or even counter-productive, or become unwell. There are likely to be differential impacts as different changes affect different groups of staff at different times. Risks are to the delivery of current work, including IfQ, and possibly technical or business continuity risks, arising from impacts on motivation, performance and effective capacity.	Clear published process, with documentation	In place – Peter Thompson	At tolerance.
	Consultation, discussion and communication, with opportunity to comment, and being responsive and empathetic about staff concerns.	Completed – Peter Thompson	
	Relatively short timeline for decision making, so that uncertainty does not linger.	In place – Peter Thompson	
	Staff kept informed of likely developments and next steps, and when applicable of personal role impacts and choices.	In place – Nick Jones	
	HR policies and processes are in place to enable us to manage any individual situations that arise.	In place – Rachel Hopkins	
	Employee assistance programme (EAP) support accessible by all. Effective line management training done for bands 4 and 3, with some band 2s also having this training now.	In place – Peter Thompson	

Organisational change combined with other pressures for particular teams could lead to specific areas of knowledge loss lasting some months (pending recruitment to fill any gaps). Such instances could affect our general capability and capacity for a period of time, and our ability to mitigate effectively against risks and issues.	Policies and processes (and the law) are in place to ensure we treat staff fairly and consistently, particularly if people are ‘at risk’. We will seek to slot staff who are at risk into other roles (suitable alternative employment).	In place – Peter Thompson
	Well established recruitment processes, which can be followed quickly in the event of unplanned establishment leavers.	In place – Rachel Hopkins
	Good decision-making and risk management mechanisms in place. Knowledge retention via good records management practice, SOPs and documentation.	In place – Peter Thompson
The above risk factors could potentially challenge our ability to complete delivery of IfQ on time.	Ability to use more contract staff if need be.	In place – Peter Thompson
Once the new structure has been agreed, there will be significant additional work involved across several teams (eg recruitment, changed ways of working, communications) to set it in place and embed it so that the benefits are realised.	Business plan discussions acknowledging that the first part of the year will include completion of IfQ and change management, so should not be loaded up too much with new work (except in teams that are relatively uninvolved in delivering IfQ or organisational change).	In place – Paula Robinson
	CMG able to change priorities or timescales in the event that this becomes necessary, in order to ensure that change is managed well.	In place – Paula Robinson
	Organisational development activity will continue, including summer awayday, to support new ways of working development	In place for coming year – Rachel Hopkins
At the start of a new business year, there are particular pressures for some teams, and for all managers (service delivery planning, Annual Report and end of year accounts, PDPs, for example). This reality plus ongoing pressures from IfQ means that implementing change at this time could be particularly difficult.	Changes will be phased in at different times, depending on factors including IfQ work and formal HR processes. Changes will not all take effect in April.	In place – Peter Thompson
	CMG remains in place and will continue to consider resources, prioritisation questions, planning, risk and performance. We have also scheduled regular informal meetings to allow managers to discuss issues arising from change, so that these can be addressed and mutual support provided.	

Additional pressure on SMT, HR and Heads, arising from the need to manage different impacts, reactions and responses in a sensitive way, while also implementing formal processes and continuing to ensure that work is delivered throughout the change period.	Recognition that change management requires extra attention and work, which can have knock-on effects on other planned work and on capacity overall. Ability to reprioritise other work if necessary.	In place – Peter Thompson
	Time being set aside by managers to discuss the changes with staff as needed, with messaging about change repeated via different channels to ensure that communications are received and understood.	In place – Peter Thompson
	SMT/CMG additional informal meetings arranged to enable mutual support of managers, to help people retain personal resilience and be better able to support their teams.	In place – Paula Robinson
Levels of service to Authority members may suffer while the changes are implemented, negatively impacting on the relationship between staff and members.	Recognition that we need to communicate the changes clearly to Authority members so that they understand when staff are implementing changes, or are particularly under pressure, and that they will have reduced capacity for a period. Members will also need to be informed when staff are new in post, and to understand that those staff need the opportunity to learn and to get up to speed.	To be implemented – Peter Thompson
Once the changes have been implemented, a number of staff will simultaneously be new in post (either new to the organisation, or in a different role). This carries a higher than normal risk of internal incidents and timeline slippages while people learn and teams adapt.	There will need to be a settling period where staff are inducted and can learn, and teams can develop new ways of working. Formal training and skills development will be provided where required. Knowledge management via records management and documentation	To be implemented – Peter Thompson
Bedding down the new structure will necessarily involve some team building time, the development of new processes, staff away days to discuss new ways of working, etc. This is essential to make the changes work well, but will be challenging to achieve given small organisational capacity and ongoing delivery of business as usual.	Change management will be prioritised so that bedding down occurs and is effective, and does not take an unduly long time.	To be implemented – Peter Thompson
	Continuing programme of leadership development for Heads and SMT.	Being planned – Rachel Hopkins

Over time, particularly once IfQ has finished, some staff may decide the changes are not for them, and that they will move on. Other staff may have different residual responses – some may fail to adapt quickly or warm to the improvements, leading to slower delivery of work and possible negative behaviours.	Processes and policies in place to manage performance and behavioural issues, recruitment, turnover, and induction of new staff, in this scenario as in any other.	In place – Peter Thompson
	The people strategy for 2017-2020 will focus on supporting and developing our staff to equip them for delivering the HFEA strategy under the new organisational model.	To be implemented – Rachel Hopkins
The new model may not achieve the desired benefits, or transition to the new model could take too long. In either case, staff could lose faith in the model and it may require adjustment later.	Management are aware of this risk, and are balancing full consideration of our needs, plus consideration of points raised by staff in the consultation exercise, with well planned phased implementation and ongoing communication throughout. The changes will be made without delay, but not all at once. Communication will be clear as to when each phase of the changes will be implemented. We will continue to explain that change will not be 'big bang' or linear. The model will be kept under review following implementation to ensure it yields the intended benefits.	To be implemented – Peter Thompson

Scoring system

The HFEA uses the five-point rating system when assigning a rating to both the likelihood and impact of individual risks:

Likelihood:	1=Very unlikely	2=Unlikely	3=Possible	4=Likely	5=Almost certain
Impact:	1=Insignificant	2=Minor	3=Moderate	4=Major	5=Catastrophic

Risk scoring matrix

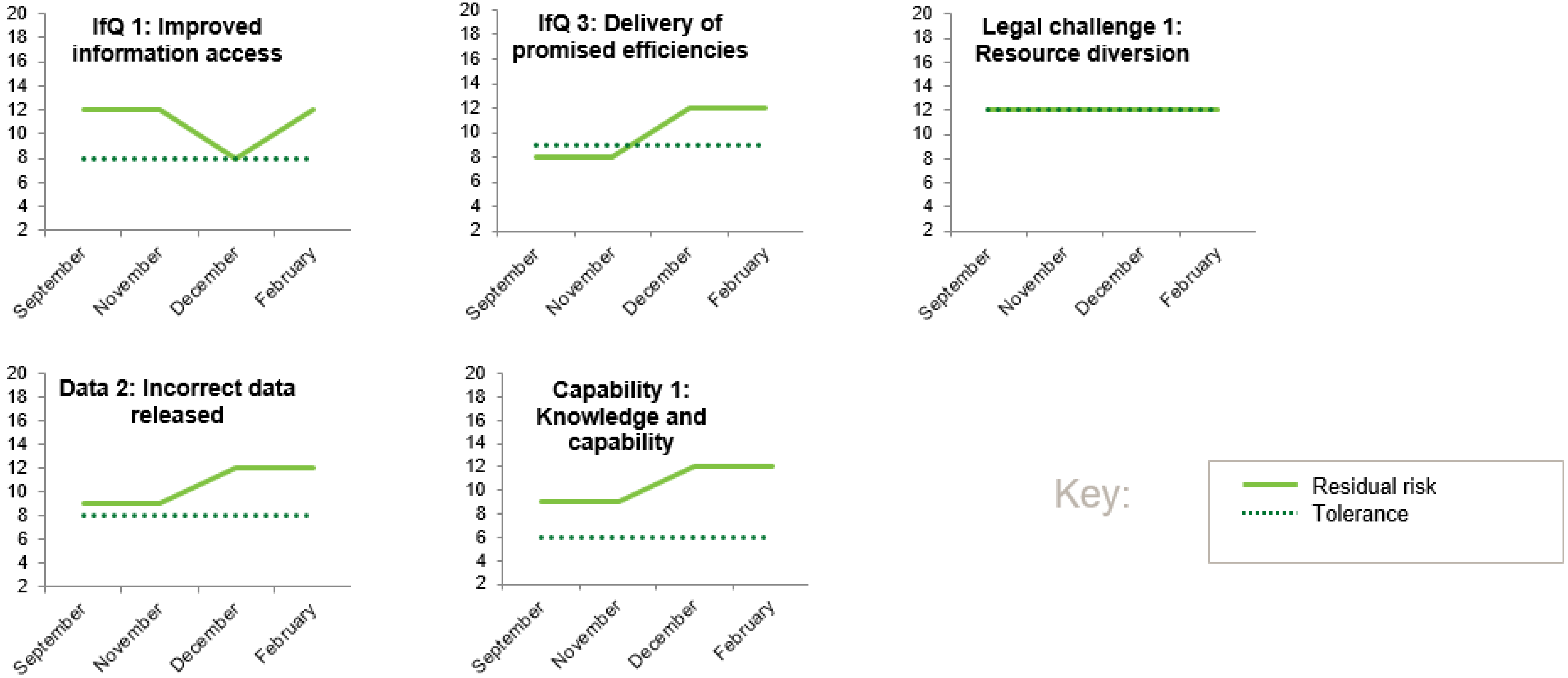
Inpact	1. Rare (≤10%)	2. Unlikely (11%-33%)	3. Possible (34%-67%)	4. Likely (68%-89%)	5. Almost Certain (≥90%)
5. Very high	5 Medium	10 Medium	15 High	20 Very High	25 Very High
4. High	4 Low	8 Medium	12 High	16 High	20 Very High
3. Medium	3 Low	6 Medium	9 Medium	12 High	15 High
2. Low	2 Very Low	4 Low	6 Medium	8 Medium	10 Medium
1. Very Low	1 Very Low	2 Very Low	3 Low	4 Low	5 Medium

Risk Score = Impact x Likelihood

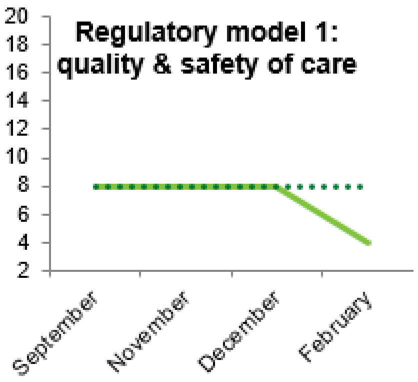
Likelihood

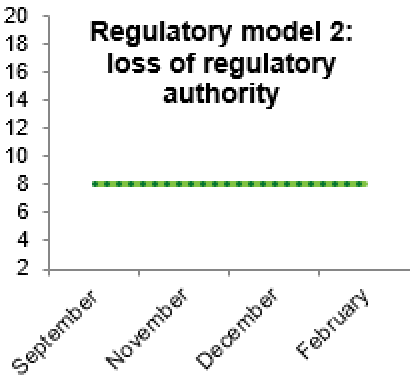
Tolerance vs Residual Risk:

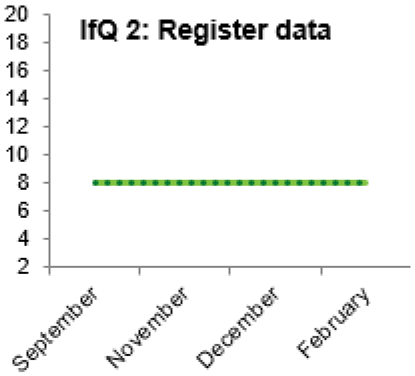
High and above tolerance risks

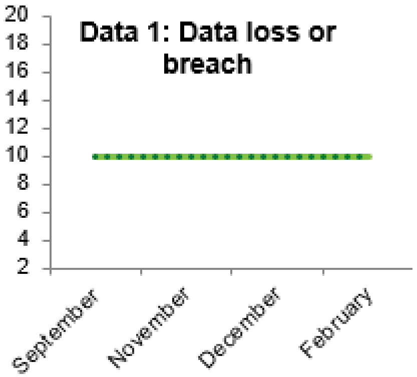


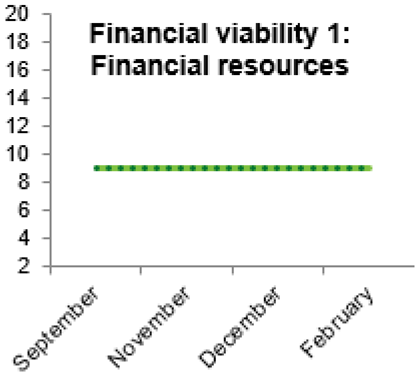
Lower level / in tolerance risks











Additional new risks:

OTR1 – Opening the Register service quality – formed from two earlier risks which can now be merged. Residual risk and tolerance both 4 (low).

OC1 – Organisational change-related instability – introduced this month, as we approach finalisation of a new organisational structure to be implemented in the new business year. Residual risk and tolerance both 9 (medium).

Information for Quality programme: update

Strategic delivery:	☒ Setting standards	☒ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item	5		
Paper number	AGC (21/03/2017) 526 NJ		
Meeting date	21 March 2017		
Author	Nick Jones, Director of Compliance and Information		
Output:			
For information or decision?	For information		
Recommendation	The Committee is asked to: • Note the Clinic Portal is now in live • Note the intention to launch the HFEA website and choose a fertility clinic as live, in April 2017 • Note the intention to 'close' the programme at the end of March 2017 • Note the arrangements for securing completion of the programme components in 2017/18		
Resource implications	The Programme budget has now been committed.		
Implementation date	During 2016–17 business year		
Communication(s)	Regular, range of mechanisms		
Organisational risk	☐ Low	☐ Medium	☒ High
Annexes:	None		

1. Background

1.1. The Information for Quality (IfQ) programme encompasses:

- The redesign of our website and Choose a Fertility Clinic (CaFC) function
- The redesign of the 'Clinic Portal' (used for interacting with clinics) and combining it with data submission functionality (Release 2) that is currently provided in our separate system (used by clinics to submit treatment data to us)
- A revised dataset and data dictionary which will be submitted for approval by the Standardisation Committee for Care Information (SCCI)
- A revised Register of treatments, which will include the migration of historical data contained within the existing Register
- The redesign of our main internal systems that comprise the Authority's Register and supporting IT processes.

1.2. Given the importance of IfQ to our strategy, we update the Committee on progress at each meeting and seek approval for direction and actions.

1.3. This paper updates Members on:

- The programme
- Work in progress – in particular, arrangements in place for data migration
- Completing the programme
- Programme budget
- Risks and issues

2. The IfQ programme

2.1. The IfQ programme is scheduled to conclude in March this year. This paper brings members up to date with progress and sets out the path to conclusion.

2.2. The programme is progressing according to 'agile' principles required by the Government Digital Service (GDS).

2.3. Our attention is now focussed on completing the work necessary to move the HFEA website from Beta to live and producing a Beta version of the treatment submission system (Clinic Portal R2) – see below.

2.4. The Clinic Portal was launched on 19 January 2017, the day following the last Authority meeting. That launch went reasonably well, albeit with some clinics getting in touch about getting access to the portal – given the enhanced security requirements. Most queries were dealt with quickly and effectively but there were frustrations felt by a few clinics. The queries were mostly categorised as 'user error' a frequently misused term: any new system will take some getting used to. Attention now is turning to the transition of the portal to business as usual status and, of course, maximising the potential of the portal as a communication channel and to drive improvements and efficiencies.

3. Work in progress

Website and choose a fertility clinic

3.1. Since the launch of the Clinic Portal, the primary focus of activity has been on completing the website. Intensive activity has been underway leading to the GDS gateway assessment for authority to live stage, which took place on 8 March 2017. We hope to be able to report the outcome of that assessment at the Authority meeting on 15 March 2017.

3.2. The team has been working very hard on creating new rich content for the website including video clips and animations as well as a home page news feed and a listings feature. We hope to demonstrate these features at the meeting.

3.3. As outlined to the Authority at the previous meeting, we had been expecting the judgment on the judicial review relating to proposals for publishing performance measures within CaFC, by the end of January 2017. To date, this has not been received, and it is still unclear when this might be received. This is obviously frustrating and at this stage we simply do not know what impact this will have on plans to launch the website.

3.4. Due to the delay to the website, and in anticipation of launch (in March/April 2017), we asked clinics (in December 2016) to undertake a verification exercise relating to their performance data in respect of CaFC. This differs from previous years' exercises (due to the new focus on cumulative birth rates) but is necessary to ensure that we can start the new CaFC with a high quality dataset (subsequent verification exercises will be more straightforward). We extended the deadline a month to the end of March 2017, to ease the burden on clinics.

3.5. Until we receive the court judgment we cannot assess the extent of any changes necessary to meet any requirements; we need to complete the CaFC verification exercise; we need to undertake security penetration testing; and we require GDS clearance. However, it is still our hope and intention to launch in April 2017.

Release 2 – data submission component

3.6. Progress on this element of IfQ has slipped because of the additional work required on the launch of the portal and the website. Section four, sets out the implications of this further. However, it is important to emphasise the foundations that have been put in place to enable us to proceed to completion over the summer.

3.7. Over the last 12 months, the Register has been subject to a thorough overhaul, and cleansing exercise. Critical data fields have been reviewed for error, absence or duplication and resolved, wherever possible. The most serious errors – so-called 'severity 1' errors – which would have prevented data migration to take place have all been resolved, thanks to the hard work of the team and clinics.

Register data migration

3.8. Data migration is planned to take place over five stages (or 'trial loads') – each 'test' migration reports on anomalies, which are fixed in advance of progression to the next test. Trial load 1 took place last year and trial load 2 has just been completed. The gaps between each get progressively shorter as the anomalies are dealt with. As expected, a number of issues were identified, and the data migration team is working productively in clearing the backlog.

3.9. As highlighted to Authority previously, we have engaged Northdoor PLC, a specialist in large-scale data migration exercises, to audit our process. The two-stage audit aims to assure the Senior Responsible Owner, the Senior Management Team and the Authority that our approach to data migration conforms with our data migration strategy and that all steps have been taken to ensure the integrity of the data being migrated.

3.10. Northdoor's preliminary audit was completed at end January 2017 and gave positive feedback on our processes. Their scrutiny was thorough and detailed, and we draw comfort from this. The second phase of Northdoor's audit is scheduled for May 2017, as we move to trial load 3 – with a final check just prior to migration.

3.11. Between trial load 1 and trial load 2 the data migration team made changes to the data to better reflect the changes in the new data dictionary. The team is currently checking that all the changes have been implemented correctly and have improved the quality of the data, as well as checking that the changes have not affected the data any unforeseen ways.

Treatment data submission system

3.12. The submission system (to be integrated within the Clinic Portal) is awaited eagerly by clinics, together with clinics using third party suppliers to link to it.

3.13. Much foundation work has taken place – including substantial user requirements' feedback; detailed mapping of all processes such that the sequencing for questions on the users' screen have been mapped; front-end designs in line with the design of the website and portal; and development activity. We are over half way towards completion but there is still much to do.

4. Completing the programme

4.1. By the end of March (the official end of the programme) a very substantial amount of our overall ambition will have been achieved. The data submission system requires completion, as noted above, and there is ongoing work to do to realise the benefits of a new system to derive intelligence.

4.2. A feature of the Programme to date has been the challenging nature of balancing so many complementary activities – the portal, website, cleansing, migration; with many components dependent on the involvement of the same individuals and skills. Since late last year our focus has been very much on completing one or more aspects to make the overall task more manageable – an approach that has been largely welcomed.

4.3. We are of the view that we need to recognise the problems of the past and configure the remainder of the work differently. To that end we will close the formal aspects of the Programme on 31 March and scope the outstanding work as a project of activity – albeit a very important one – within our business plan commitments for 2017-18. It will be very important that we do not conflate the closure of the programme with any dilution of our commitment to deliver the final elements. Our stakeholders will demand nothing else.

4.4. Such an approach also fits with our plans for organisational change currently being discussed with staff, and with our expectations as regards budget and capital allowances – both consistent with our longer-term expectations to support a new IT estate. Further detail in relation to this will be presented at the meeting.

5. Programme budget

5.1. Our IfQ budget this year 2016-17 was £527,000 (revised upwards to £619,00 in May 2016) within an overall revised budget for 2015-17 of £1.227m. Projections to year end are that expenditure will be slightly below this.

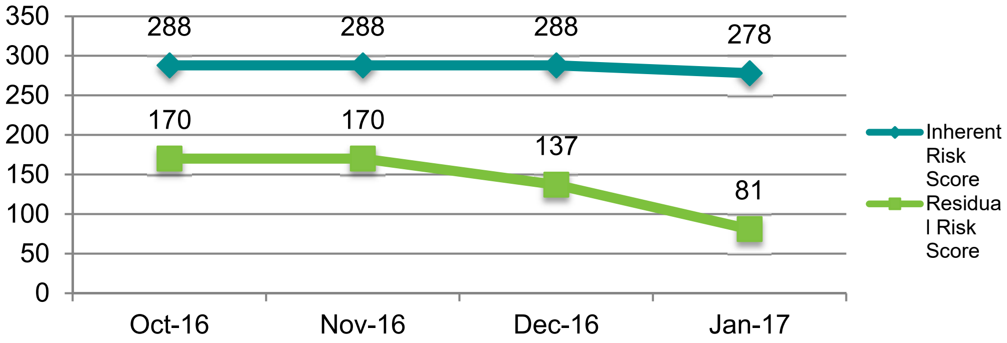
5.2. We have now concluded our contractual commitments to Reading Room, our principal external supplier. We spent a little time in January and February agreeing the final schedule of work, which resulted in our requiring them to complete a slightly smaller amount of work, resulting in a contract underspend of just under £30,000 – which we have reallocated to other priorities – to ensure that we complete as much work as possible relating to R2 the data submission system, this financial year. To this end we have secured the services of three independent contractors to the end March 2017.

5.3. The earned value and spend to date have progressed slightly, this is reflecting the final stage of the programme for both portal and websites, although the portal has gone live critical work remain to be done for the website.

Period	Aug-16	Sep-16	Oct-16	Nov-16	Dec-16	Jan-17
Earned Value	86%	88.5%	90.6%	91.1%	91.9%	92.3%
Spend to date	91%	92.1%	92.9%	93.1%	93.2%	93.2%

6. IfQ risks and issues

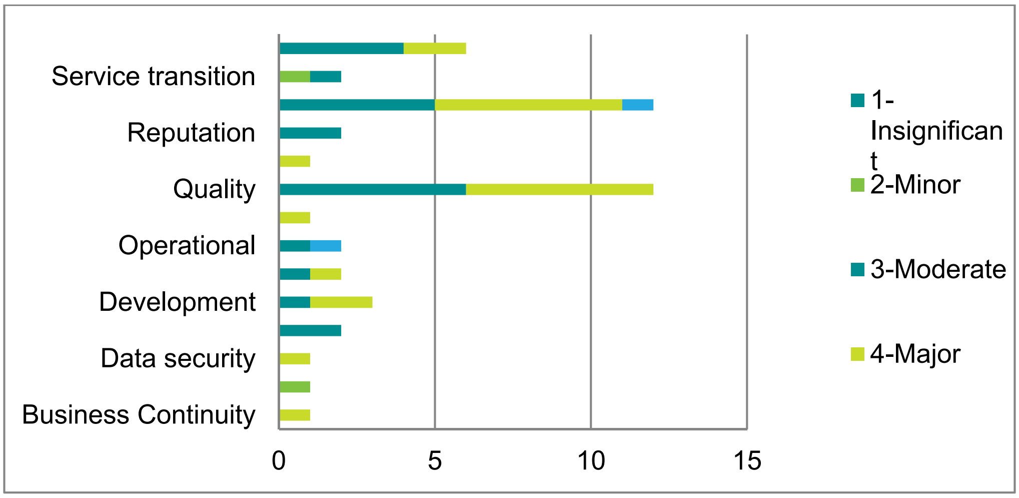
6.1. The below line graph represents the overall IfQ risk score, which combines the perceived impact and likelihood of the current risks on hand each month. A number of the risks have been reviewed and updated in the last month and the risk scores, both inherent and residual, have decreased.



6.2. In addition to IfQ-specific risks, the Corporate Management Group has also recently reviewed the strategic risk register, and added a risk relating to the organisational changes that will be implemented over the coming months. There is a potential risk to the delivery of release two, arising from the impact of the changes on key teams.

6.3. The IfQ risk log will continue to be monitored and updated over the next month, as will the impacts of the organisational restructuring, as these play out over time.

6.4. The major risks are associated with resources, timescales, regulatory monitoring, quality, financial, development, patient information, data security and business continuity.



7. Recommendation

7.1. The Committee is asked to:

- Note the Clinic Portal is now in live
- Note the intention to launch the HFEA website and choose a fertility clinic as live, in April 2017
- Note the intention to 'close' the programme at the end of March 2017
- Note the arrangements for securing completion of the programme components in 2017/18.