Audit and Governance Committee meeting - agenda

5 December 2017

Abbey Room

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

	Agenda item		Time
1.	Welcome, apologies and declaration of interests		10:00am
2.	Minutes of 3 October 2017 **[AGC (05/12/2017) 571]**	For Decision	10.05am
3.	Matters Arising **[AGC (05/12/2017) 572 MA]**	For Information	10.10am
4.	Regulatory and Register Management **[AGC (05/12/2017) 573 NJ]**	Presentation	10.20am
5.	Internal Audit a) Progress Report **[AGC (05/12/2017) 574 DH]** b) Risk Management Final Report **[AGC (05/12/2017) 575 DH]**	 For Information For Information	10.50am
6.	Implementation of Audit Recommendations **[AGC (05/12/2017) 576 MA]**	For information	11.00am
7.	External Audit – Audit Planning Report **[AGC 05/12/2017) 577 NAO]**	Verbal Update	11.05am
8.	Handling Brexit **[AGC 05/12/2017) 578 PT]**	Presentation	11.15am
9.	Digital Programme Update: Including Data Submission **[AGC ((05/12/2017) 579 NJ]**	For Information	11.35am
10.	Resilience, Business Continuity Management and Cyber Security **[AGC (05/12/2017) 580 DH]**	For Information	11.50am

11.	Strategic Risk Register **[AGC (05/12/2017) 581 HC]**	For Discussion	12.00pm
12.	AGC Forward Plan **[AGC (05/12/2017) 582 MA]**	For Decision	12.30pm
13.	Whistle Blowing and Fraud **[AGC (05/12/2017) 583 RS**	Verbal update	12.35pm
14.	Contracts and Procurement **[AGC (13/06/2017) 584 MA]**	Verbal update	12.45pm
15.	Any other business		12.55pm
16.	Close (Refreshments & Lunch provided)		1.00pm
17.	Session for members and auditors only		1.00pm
18.	Next Meeting 10am Tuesday, 6 March 2018, London		

2.00pm –Training session for members - Cyber security and information Risk Guidance for Audit Committees

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 (05/12/2017) 571		
Meeting date	5 December 2017		
Author	Bernice Ash, 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 3 October 2017

HFEA Offices, 10 Spring Gardens, London SW1A 2BU

Members present	Anita Bharucha (Chair) Margaret Gilmore Mark McLaughlin Geoffrey Podger
Apologies	Morounke Akingbola, Head of Finance
External advisers	Internal Audit - PricewaterhouseCoopers (PwC): Jeremy Nolan External Audit - National Audit Office (NAO): Sarah Edwards George Smiles
Observers	Kim Hayes, Department of Health
Staff in attendance	Peter Thompson, Chief Executive Juliet Tizzard, Director of Strategy and Corporate Affairs Richard Sydee, Director of Finance and Resources Nick Jones, Director of Compliance and Information Paula Robinson, Head of Planning and Governance Helen Crutcher, Risk and Business Planning Manager Dan Howard, Chief Information Officer Bernice Ash, Committee Secretary

1. Welcome, apologies and declarations of interests

1.1 The Chair welcomed attendees to the meeting, in particular, new Committee members Mark McLaughlin and Geoffrey Podger. The Chair also welcomed Dan Howard, Chief Information Officer, to the meeting.

1.2 The Chair formally thanked Gill Laver and Jeremy Page, who attended their last meeting on 13 June 2017, for their contributions to the Committee. The Chair confirmed that a letter of thanks had been sent to both individuals.

1.3 Apologies were received from Morounke Akingbola, Head of Finance.

1.4 There were no declarations of interest.

2. Minutes of the meeting held on 13 June 2017

2.1 The minutes of the meeting held on 13 June 2017 were agreed as a true record and approved for signature by the Chair.

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 Items 4.7, 8.11, 9.8, 11.8, 11.9 and 14.4 relating to Strategy and Corporate Affairs Management, internal audit, IfQ, fraud and business continuity, resilience and security have been addressed in the items on the agenda below.

3.3 3.6) Staff had noted that it would be useful for a message to be sent to members' private email addresses, informing them of any new information sent to their HFEA accounts. The Committee agreed this item could be removed from the matters arising log.

4. Internal Audit

Progress Report

4.1 The Head of Internal Audit provided the Committee with an update on progress against the current internal audit plan. The Committee noted that the final internal report for the data loss review was issued a moderate rating. The outcome of this audit had given a broadly positive picture, with some areas requiring tightening, but with no major areas of concern regarding current practice.

4.2 The Director of Compliance and Information reported that the data loss exercise had been useful and anticipated the Authority having more oversight of clinics' data security in future; this would be assisted by the fact that the Chief Information Officer was now in post. The Committee was also informed there would be a new Senior Inspector post, focusing on working with clinics and other inspectors to improve practices regarding data.

4.3 The Head of Internal Audit stated more work needs to be conducted on information governance in clinics and the Director of Compliance and Information confirmed that a new data submission process for them would be developed, including checklists, updating SOPs and improving standards. The Director of Strategy and Corporate Affairs confirmed that a new Information Policy would be developed in 2018, alongside an Intelligence Strategy.

4.4 The Chair welcomed the addition of the General Data Protection Act to the internal audit plan. The Committee noted that, as this area had been added to other organisations' plans, there was the future potential to benchmark this particular audit.

4.5 The Committee noted that the report stated, 'there was no management assurance documented to demonstrate that all HFEA staff have completed the mandatory e-learning 'responsible for information training''. It was identified that there is mandatory e-training, as part of the induction process, for new Committee members and the Authority was asked to ensure all new, and established members, receive this regularly.

4.6 The Committee confirmed they would welcome the production of a three-year plan. The Director of Finance and Resources stated this could comprise of four or five specific audits, but also have scope to be flexible and adaptable.

Action

4.7 The Director of Compliance and Information and the Head of Planning and Governance to ensure all new, and established, Authority and Committee members receive the mandatory e-learning 'responsible for information training' regularly.

5. Strategy and Corporate Affairs Management

5.1 The Director of Strategy and Corporate Affairs spoke to a presentation regarding the 2014-2017 Strategy, the 2017-2020 Strategy, changes in the Directorate and potential risks.

5.2 The Director of Strategy and Corporate Affairs reported on the standards achieved with regards to the 2017 Strategy. The launch of the new website had been challenging, but it now enabled the provision of valuable information through its 'Choose a Fertility Clinic' function and a new tool which allowed patients to give feedback on their experience of care. It was noted the work on publishing more data to drive improvements in clinic performance and improving treatment success rates remained outstanding.

5.3 The Committee noted the work conducted on the experience of donor conception and addressing the misconception that patients must go overseas for treatment. The Director of Strategy and Corporate Affairs reported that work with donor conception patients and donors is ongoing.

5.4 Work on increasing and informing choice had been achieved through the presentation of clinic information on the website, and work with NHS England on commissioning the best services continues. Improved information about treatment and research, user experience scores and collaboration with professionals about giving information and advice at the right time had been achieved. More work needs to occur to ensure clinics prepare patients and donors well through their provision of information.

5.5 The Director of Strategy and Corporate Affairs provided an overview of the three strands within the 2017-2020 Strategy concerning safe, ethical, effective treatment, consistent outcomes and support, alongside improving standards through intelligence, which is a new area for the Authority.

5.6 The Committee noted the new structure of the Strategy and Corporate Affairs Directorate, comprising four areas; planning and governance, communications, regulatory policy and the recently formed intelligence team.

5.7 The Committee was provided with a summary of the Directorate risk trends from 2015 to 2017, highlighting the constant risk of litigation and becoming distracted by external challenge. The need to maintain our reputation as a robust and trusted regulator was noted. The Director of Strategy and Corporate Affairs referred to the skilled handling of the investigation into poor practice in some fertility clinics by the Authority.

5.8 The Director of Strategy and Corporate Affairs stated that the Authority has established good stakeholder relations within the sector and the next phase needs to involve the 'power of persuasion' as opposed to solely using policy levers, alongside empowering patients to ask questions.

5.9 The Committee expressed some concern regarding the Authority's reputation risk, with particular regard to PGD, which had an increasing number of grey areas and complex decisions. This could result in more legal challenges. The Chief Executive spoke of the tensions with regards to legal

challenges, stating that Judicial Reviews are usually challenges concerning process, not policy. The need to ensure that good practice is spread throughout the Authority and clinics was acknowledged.

5.10 The Committee discussed the potential impact and opportunities resulting from the UK's forthcoming exit from the European Union, questioning whether clinics are ready to deal with the issues resulting from this. This is a major issue of concern for the Department of Health and will need to be covered with the Authority, in due course, when more clarity from government is received.

5.11 Capacity issues had also been identified as a risk trend and the need for staff to become more agile, testing potential new processes prior to full implementation, was noted. Reasoned decisions needed to be made about the level of quality required of a given product, since quality needed to be balanced against cost and resources and the speed of delivery.

5.12 The Committee felt that the risk of external challenge should be thought of as part of normal business as opposed to a distraction. The Chair noted there has been a period within which the Authority needed to justify elements of its work.

5.13 The Committee thanked the Director of Strategy & Corporate Affairs for an excellent presentation that had prompted valuable discussion.

6. External Audit – Audit Planning Report

6.1 The NAO provided an update on the audit planning report, highlighting the significant risk identified and the proposed risk approach. They noted that whilst they do not consider it a significant risk they will monitor the Authority Judicial Review case. The Committee noted the risk assessment.

6.2 The Committee noted the timetable of work, fees and the audit approach, The NAO also referred to other matters that have been considered as part of the risk assessment but were not anticipated to raise a risk to the financial statements, for example data submission, portal expenditure, fraud, the recent egg sharing investigation and Brexit.

6.3 The NAO informed the Committee that a new Letter of Understanding would be issued shortly.

6.4 The Chair noted that training for Committee members, linked to the meeting cycle, had been discussed previously and – with the arrival of new members – it would be timely to institute this. The Director of Finance and Resources would create a training plan for the Committee, ensuring sessions are scheduled to occur on the same dates as planned meetings.

Actions

6.5 NAO to update the current wording, regarding fraud, in the audit planning report and re-issue for inclusion in the published committee papers.

6.6 The Director of Finance and Resources to create a training plan for the Committee, ensuring sessions are scheduled to occur on the same dates as planned meetings.

7. Data Submission Project (formerly IfQ)

7.1 The Director of Compliance and Information spoke to the paper and presentation, providing information on the data submission project (formerly IfQ).

7.2 The Committee was informed that feedback on lessons learned from IfQ will be provided at the 5 December meeting. The budget for completion of the data submission project has been established at £350,000 and the launch date has been set at 1 April 2018.

7.3 The Committee noted that following the launch of the website in June 2017, the IfQ programme had closed and the data submission project had commenced. This project entails work on a revised dataset and dictionary, a revised Register of treatments, including the migration of historical data, redesign of the system many clinics use for treatment data and to enable clinics using third party patient record systems to make submissions from these to the Authority's Register.

7.4 The Director of Compliance and Information reported that work on an Information Policy for clinics has commenced alongside cleansing of their data. The purpose of this work is to enhance the Register migration and provide clinics with a better front-end experience.

7.5 The Committee noted that user testing with representatives from six clinics, to check user experiences with screen navigation, design and fit with clinic business processes, took place on 21-22 September 2017. The feedback from this testing was entirely positive and clinic staff were enthusiastic for implementation to occur.

7.6 Key risks and issues for the project concerning data migration activity and third-party suppliers were identified. The Director of Compliance and Information stated there are no shortcuts for conducting this project work since all treatment records need to be migrated to a new people-based database structure, which is complex. The difficulty of extracting progress metrics on this work was discussed, but fortnightly catch-ups on progress should assist.

7.7 The Committee was informed that the Authority had engaged with the third-party suppliers used by some clinics. The importance of managing supplier and clinic relationships was noted.

7.8 The Committee had some discussion surrounding the Authority's capability and capacity to maintain the system, once the migration and launch is completed. The Director of Compliance and Information stated there is a prototype working system and he has confidence that it can maintained technically in-house.

7.9 The Chief Information Officer stated it was a challenge to ensure the correct staffing infrastructure is in place, but provided assurance it can be achieved. The project staffing matrix can be revised, if there is any slippage, so to meet the 1 April 2018 launch date. Should the project go beyond this date, Department of Health capital approval would be required and there would also be a reputational risk.

7.10 The Chief Executive stated that all energies are being concentrated on this project and that the SMT was determined for the completion of the project to be by the end of the 2017/2018 year. The only caveat was that data migration would not take place until it was clear that the Register data was not at risk.

7.11 The Committee noted that different data has different tolerance levels and that greater clarity is required on data metrics so that progress is clearer. The Director of Compliance and Information assured the Committee that such detail will be available for the 5 December 2017 meeting. The

Chair stated the importance of knowing the risk, and the level of risk. It was agreed that the Committee should be provided with a progress update on the data submission project before the next Authority meeting in November.

Action

7.12 The Director of Compliance and Information to provide the Committee with a progress update on the data submission project, based on clear metrics, before the next Authority meeting in November.

8. Resilience and Business Continuity Management and Cyber Security

8.1 The Chief Information Officer spoke to the paper and presentation, informing the Committee of the Business Continuity test which occurred on 20 September 2017. This was largely successful, with some improvements required for smartphone access. A tabletop test took place on 27 September 2017 and results from this suggested that plans and contingencies are robust, but some work is needed on contact details for the core response team and other updates to the policy. Authority members would be sent an email with a link for testing the business continuity site, asking for feedback to be provided on any issues arising.

8.2 The Committee was informed of the Chief Information Officer's team priorities, noting that the vacancies for the IT Services and Systems Manager and Lead Developer would be advertised externally within the week. The production of a new IT/Digital Strategy was also identified.

8.3 The Committee raised concern about their levels of access to Office 365, highlighting the importance of having the capacity to view this for business continuity purposes. It was crucial that all new and existing Committee members have access to O365 set up quickly, with the correct permissions.

8.4 The committee also discussed the need to ensure the contact details for all staff were kept updated, and website resources which could help raise awareness of all aspects of cyber security.

Action

8.5 The Chief Information Officer to ensure all new and existing Committee members have access to O365 set up quickly, with the correct permissions, including the ability to view the business continuity SharePoint site in O365.

9. Strategic Risk Register and Legal Risks

9.1 The Risk and Business Planning Manager presented the Strategic Risk Register.

9.2 The Committee was informed the Strategic Risk Register now contained seven risks, with two currently above tolerance - these were the risks regarding capability and organisational change. Due to the 2017/18 version of the Risk Register being updated to include risk areas in a slightly different format to previously, the new risks of cyber security, regulatory effectiveness and effective communications do not yet have four trend points.

9.3 The Risk and Business Planning Manager informed the Committee that the risk level for legal challenge had abated since the last meeting due to an absence of matters at the time the Register was reviewed.

9.4 The Committee was informed that the top-level description of the regulatory effectiveness and messaging and engagement risks had been altered since the meeting on 13 June 2017. Wider external system-wide interdependencies continue to be reported under each risk.

9.5 The Chief Executive spoke about the capability and organisation change risks, explaining how IfQ and the new 2017-2020 strategy has impacted on these. Due to the new structure for IT, some existing staff did not hold the necessary skills required and have therefore been part of a small redundancy scheme. Some staff have left the Authority over the Summer period, with others departing before the end of 2017; this would conclude the planned redundancies.

9.6 The Chief Executive also spoke of the challenges posed by unplanned change at the Authority, with regards to other experienced members of staff leaving the organisation. The long-term restrictions on public sector pay are a factor. The Committee was informed that more staff events eg, Away Days and a refresh of the People Strategy were planned to help with staff engagement.

9.7 Legal challenge had been an area of concern but seemed fairly controlled at present. The Chief Executive stated that some judgements on consent in legal parenthood remain outstanding, but the number of cases has slowed down. The Authority had won the Judicial Review case concerning the IfQ Choose a Fertility Clinic project, but a decision from the Court of Appeal on whether permission to appeal should be granted is still awaited. It was noted that a licensing matter is currently being challenged and will be considered by the Appeal Committee in October 2017. This matter is also subject to a Judicial Review which is stayed awaiting the outcome of the appeal.

9.8 The Risk and Business Planning Manager gave the Committee an explanation of ‘above tolerance’ and how the desired tolerance level is reached for the individual risks. The Committee commended the quality of the Strategic Risk Register, suggesting it would be useful for further explanation of the tolerance levels to be added. The concepts of risk tolerance and risk appetite should also be explained in the HFEA’s risk policy.

9.9 The Committee felt there is currently insufficient governance with regards to cyber security. It is important to ensure that the Authority member responsible for cyber security is informed of any issues. The importance of ensuring all staff receive cyber security training was also highlighted.

9.10 The Committee thanked staff involved in the preparation of the Risk Register for the clear presentation of risks, which enabled members to focus on the key issues.

Actions

9.11 To ensure that the Authority member responsible for cyber security is informed of any issues.

9.12 To ensure all staff receive cyber security training.

9.13 The Risk and Business Planning Manager to update the Strategic Risk Register to include an explanation of the tolerance levels.

10. Reserves Policy

10.1 The Director of Finance and Resources spoke to the Committee on the financial Risk Policy, particularly highlighting the contingency in cashflow and the need to approach the Department of Health should there be any significant financial issues with regards to a legal challenge.

10.2 The Committee discussed possible uses for surplus monies including to help fill staff gaps and the data migration project. The Director of Finance and Resources confirmed there is £600,000 retained for legal costs, should it be required.

10.3 Levels of cash balance were discussed and it was noted that clinics are not keen to move away from the cost per cycle model and welcome stability in our pricing. The Chief Executive reported that work was ongoing to review our approach to forecasting and setting fees.

11. AGC Forward Plan

11.1 The Committee noted that the theme for the 5 December 2017 meeting would be business continuity, the Register and compliance.

11.2 The Chair noted that a review of the Committee's activities, effectiveness and terms of reference was listed for discussion at the 5 December 2017 meeting, suggesting the possibility of deferring this item to a later date, enabling more time for the new members to embed into the Committee. The Head of Planning and Governance would investigate whether a deferral of this item would have any implications for other Authority business (such as the annual review of Standing Orders), and confirm with the Chair.

Action

11.3 The Head of Planning and Governance to investigate whether a deferral of the item on activities, effectiveness and terms of reference, from the 5 December 2017 Committee meeting, would have any implications for other Authority business and confirm with the Chair.

12. Whistle Blowing and Fraud

12.1 The Director of Finance and Resources informed the Committee that the case of alleged fraud in connection with a contract provider is still under investigation with the DH Anti-Fraud team. The HFEA is relatively hopeful it would not suffer any financial losses in relation to this case. The Committee would be updated in due course.

13. Contracts and Procurement

13.1 The Director of Finance and Resources reported there were no issues, new contracts let or procurement to report since the last meeting.

14. Any Other Business

14.1 Members and auditors retired for their confidential session.

14.2 The next meeting will be held on Tuesday, 5 December 2017 at 10am.

15. Chair's signature

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

Signature

Name

Anita Bharucha

Date

5 December 2017

Audit and Governance Committee Paper

Paper Title:	**Matters arising from previous AGC meetings**
Paper Number:	**[AGC (05/12/2017) 572 MA]**
Meeting Date:	5 December 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:

- 9 items added from October 2017 meeting, 6 ongoing
- 3 items carried over from earlier meetings, 2 ongoing

ACTION	RESPONSIBILITY	DUE DATE	PROGRESS TO DATE
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**
Matters Arising from Audit and Governance Committee – actions from 13 June 2017 meeting			
8.11 The Director of Finance and Resources to explore the potential to surplus funds to commission research on the data held by the Authority.	Director of Finance and Resources		**Completed**
15.2 The Director of Finance and Resources to ensure the Committee remains updated with regards to the outcome of the investigation	Director of Finance and Resources		**Ongoing** - An update will be provided at the December 2017 meeting
Matters Arising from Audit and Governance Committee – actions from 3 October 2017 meeting			
4.7 The Director of Compliance and Information and the Head of Planning and Governance to ensure all new, and established, Authority and Committee members receive the mandatory e-learning 'responsible for information training' regularly**.**	Director of Compliance and Information and the Head of Planning and Governance		**Ongoing -** An update will be provided at the December 2017 meeting
6.5 NAO to update the current wording, regarding fraud, in the audit planning report and re-issue for inclusion in the published committee papers.	NAO		**Completed**

6.6 The Director of Finance and Resources to create a training plan for the Committee, ensuring sessions are scheduled to occur on the same dates as planned meetings.	Director of Finance and Resources		**Ongoing -** An update will be provided at the December 2017 meeting
7.12 The Director of Compliance and Information to provide the Committee with a progress update on the data submission project, based on clear metrics, before the next Authority meeting in November.	Director of Compliance and Information		This is covered under agenda item 9
8.5 The Chief Information Officer to ensure all new and existing Committee members have access to O365 set up quickly, with the correct permissions, including the ability to view the business continuity SharePoint site in O365.	Chief Information Officer		**Ongoing -** An update will be provided at the December 2017 meeting
9.11 To ensure that the Authority member responsible for cyber security is informed of any issues.	Chief Information Officer		**Ongoing**
9.12 To ensure all staff receive cyber security training.	Chief Information Officer		**In progress -** Staff have been made aware that training is being planned.
9.13 The Risk and Business Planning Manager to update the Strategic Risk	Risk and Business Planning Manager		**Completed -** An update will be provided at the December 2017 meeting

Register to include an explanation of the tolerance levels.			
11.3 The Head of Planning and Governance to investigate whether a deferral of the item on activities, effectiveness and terms of reference, from the 5 December 2017 Committee meeting, would have any implications for other Authority business and confirm with the Chair	Head of Planning and Governance		**Completed** - Head of Planning and Governance has confirmed with Chair this can be deferred from the 5 December 2017 meeting,

Audit and Governance Committee

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

Details:	
Meeting	Audit & Governance Committee
Agenda item	5b
Paper number	AGC (05/12/2017) 574
Meeting date	5 December 2017
Author	Jeremy Nolan

Output:	
For information	To provide an update to the Audit and Governance Committee on progress against the current Internal Audit plan.
Progress Update	Good progress is been made against the agreed plan. The final report for HFEA Risk Management was issued on the 29th November, with the review awarded a Moderate rating. The fieldwork has also commenced on the Financial Controls and .Preparation for the General Data Protection Regulations reviews, with final reports expected to be issued in January 18. Work on the recommendation follow up review is also expected to commence in early December.
Actions from previous meeting	1) Jeremy to provide a verbal update on Cyclical Audit planning from 2018/19 onwards
Organisational risk	☐ Low ☒ Medium ☐ High
Annexes	Annex A - Progress against the latest iteration of the HFEA Internal Audit plan 2017/18 Annex B - The Final Report for Risk Management review, which has been given a MODERATE assurance rating.

Annex A

HUMAN FERTILISATION & EMBRYOLOGY AUTHORITY INTERNAL AUDIT PLAN 2017/18

Audit Ref No	Audit Title	Audit Review Detail	Directorate/Grouping	Current Status (25/9/17)	Quarter Review Due to Start	Days Indic' and Agreed	Notes
1	Data Loss	This audit will review the controls around the key risk that HFEA data is lost, becomes inaccessible, is inadvertently released or is inappropriately accessed.	Compliance & Information	Final Report	Q1	13	As agreed at the June Audit and Governance Committee meeting, extra days were moved to this review, from the Risk Management audit. Final report issued on 25th September.
2	Risk Management and Governance	Overview of general governance, risk management and assurance arrangements. Review will focus on ensuring there is a formal governance structure in place, that key risks are identified, that they are reflected accurately within the assurance framework and are a key focus for the HFEA Board.	Strategy and Corporate Affairs	Final Report	Q2	7	Final report issued on the 29th November.
3	Financial Controls	This is a standard key financial controls review. We will identify and review key financial processes and controls operated by HFEA as well as consider any potential overlaps with HTA.	Finance & Resources	Fieldwork	Q3	10	Audit to be aligned with HTA audit. Fieldwork commenced on the 22nd November.

4	General Data Protection Regulation	This will consider the state of preparations for the introduction of this regulation in May 2018. An audit at this stage will be useful to give assurance to the Audit and Governance Committee and to give time for any recommendations to be implemented.	Compliance and Information	Fieldwork	Q3/Q4	10	Audit to be aligned with HTA audit. Fieldwork commenced in early November.
5	Follow up recommendations	Follow up of agreed recommendations of previous Audits. A summary of findings and results to be presented at each ARC	Various	Not started	Q3/Q4	5	Fieldwork to commence in early December.

Risk Management Final Report

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 (05/12/2017) 575 DH		
Meeting date	05 December 2017		
Author	Jeremy Nolan		
Output:			
For information or decision?	For information		
Recommendation	The Committee is asked to note: • This report and its recommendations		
Resource implications	None		
Implementation date	During 2017–18		
Communication(s)			
Organisational risk	☐ Low	☐ Medium	☐ High
Annexes:	None		

Health Group Internal Audit

Reference number: DHX 217 008 003
FINAL REPORT
HUMAN FERTILISATION & EMBRYOLOGY AUTHORITY
NOVEMBER 2017

Report Name: Risk Management

Overall report rating: MODERATE

Health Group Internal Audit, part of the Government Internal Audit Agency (GIAA) 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 6083
1N16 Quarry House, Quarry Hill,
Leeds, LS2 7UE

CONTENTS PAGE

Date fieldwork completed:	11th October 2017
1st draft report issued:	16th November 2017
Management responses received:	28th November 2017
2nd draft report issued:	N/A
Management responses received:	N/A
Final report issued	29th November 2017

Report Author: Tony Stanley
Version №: FINAL

Distribution List – Draft Report

Main recipient(s)

Paula Robinson	Head of Planning and Governance
Juliet Tizzard	Director of Strategy and Corporate Affairs

cc:

Richard Sydee	Director of Finance & Resources
Nick Jones	Director of Compliance and Information
Tony Stanley	HFEA Deputy Head of Internal Audit
Jeremy Nolan	HFEA Head of Internal Audit
Cameron Robson	Group Chief Internal Auditor

Distribution List – Final Report

As for draft report.

EXECUTIVE SUMMARY

1. Introduction

1.1 The Human Fertilisation & Embryology Authority (HFEA) is the regulator of fertility treatment and human embryo research in the UK. The role of the organisation includes licensing of clinics, setting standards and checking compliance with them through inspections. HFEA also plays a public education role by providing information about treatments and services for the public, people seeking treatment, donor-conceived people and donors. HFEA's role is defined in law by the Human Fertilisation and Embryology Act 1990 and the Human Fertilisation and Embryology Act 2008.

1.2 Robust risk management is fundamental to an effective and well managed public sector body, supporting it to achieve its objectives. To help support the management of risk, HFEA have in place an Audit and Governance Committee which oversees corporate governance, risk, audit arrangements and financial matters.

1.3 The objective of this audit was to review the risk management arrangements within HFEA, focusing on one of the seven risks currently on the strategic risk register. It was agreed with management that a 'deep dive' review of the Capability risk would be the most appropriate area to review and would add the most value at this time. The review looked at the adequacy and effectiveness of the controls that HFEA currently have in place to manage this risk.

1.4 Our fieldwork involved interviews, including the Head of Planning and Governance, attendance at a HFEA Corporate Management Group Risk meeting and a review of all HFEA policies and guidance documents, which are linked to risk management and corporate governance.

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 governance, risk management and control.

2.2 To support our overall opinion, we have identified positive evidence of good practice in managing the capability risk, and this is detailed in paras 3.2-3.9. However, we also found, at the time of our fieldwork, that there are areas for improvement in the HFEA risk management framework, the most significant issue (with a recommendation assessed at 'medium' level) being the inconsistency in the information captured within the strategic risk register

3. Summary of Findings

3.1 Our overarching finding is that HFEA has a robust risk framework in place which supports and promotes a good risk management culture. Senior management have put solid foundations in place, including the production of a risk management policy, which clearly sets out HFEA's approach to risk management, and outlines procedures, roles and responsibilities and the treatment of risk.

3.2 HFEA has a corporate risk register in place, which contains seven strategic risks, all of which have been agreed by HFEA senior management team as having either high or medium risk. Beneath this there are also operational risk registers across all teams within HFEA. These frameworks are what we would expect to be in place in a good risk management environment and are aligned with good practice guidance. We also found the following positive evidence on the key scope areas reviewed during our 'deep dive' of HFEAs Capability risk:

3.3 **Risk Ownership**: There is clear ownership of the capability risk, with the HFEA Chief Executive having overall responsibility. The risk is separated into several sub-categories, each assigned an individual owner from the senior management team. Each owner provides an update on their particular risk area at each meeting of the Corporate Management Group (CMG). The CMG is attended by the Chief Executive, directors and section heads, which provides a strong level of accountability. We consider this to be in line with good practice.

3.4 **Risk Assessment:** Risks are assessed using a five point rating system assessing likelihood and impact, with both an inherent risk rating and residual risk rating once controls have been taken into consideration. The rating is discussed and agreed at each CMG meeting, with ongoing commentary provided to justify the rating agreed and any changes made. Each of the capability sub risks include documented mitigations, with updates provided on any key issues likely to have any impact on the overall rating.

3.5 **Staff Turnover/Knowledge Retention:** This is discussed regularly at CMG, which ensures that these issues are high on the radar of the senior management team, and re-prioritisation of work is discussed to alleviate any short term staffing issues. Prior to staff leaving or going on planned long term absence, there are procedures in place to ensure knowledge is captured. This is done via structured handovers, manager engagement and ensuring all key documentation is filed appropriately.

3.6 **Decreased effectiveness/Performance failures:** Performance and prioritisation of work are standing agenda items at CMG meetings. HFEA carried out a wide staff consultation on an organisational change document in early 2017 to gauge staff views on various issues. This resulted in a refined version of the new organisational model. In addition to this a people strategy has also been drafted (and is now near-final) which sets out HFEA's core principles. This is supported by a set of commitments from senior management on leadership, culture, engagement, performance and development. We consider this to be a positive initiative, however at the time of the audit the strategy and commitment had not been published to all staff. HFEA also have a suite of detailed HR policies and procedures to support staff, and access to an employee assistance programme is available to all.

3.7 **Current and future resource issues:** HFEA have good systems in place to monitor both staff levels and absence levels, with reports routinely produced and presented at CMG for discussion. At the time of the review the register team were at full capacity, and the risk has reduced as staff increase their capability. Temporary staff recruitment is used to ensure continuity of activity and ensure there are no back logs of work.

Regular surveys are used by HFEA to capture all views of staff and try to identify areas for improvement.

3.8 **Technical Issues:** A new Chief Information Officer (CIO) joined HFEA in September 17, and one of the main priorities is to improve long standing issues with SKYPE communication, which have been ongoing since 2016. External venues are also being used to help mitigate the issue, with a new switchboard system being implemented during the course of the audit fieldwork.

3.9 Whilst the audit work provides assurance that there is a good risk management framework, we consider that there are areas where improvements could be made:

3.10 **Strategic Risk Register:** The current strategic risk register used to inform senior management meetings should be updated to ensure it is more comprehensive, ensures that all stated mitigations include effective controls to reduce the level of risk, includes details of the contingency arrangements in place and also clearly details HFEA's risk tolerance.

3.11 **Staff Turnover**: At the time of the audit staff turnover was above the agreed key performance indicator for HFEA, which has the risk of impacting on business as usual activity. We acknowledge that HFEA have taken action to identify the root causes behind this turnover, including staff surveys and exit interviews, and that a pay comparison document had been produced and circulated to staff.

3.12 We have also raised some other points for management to consider, although these are 'observations' rather than recommendations and are intended to add value.

- Consideration should be given to running a series of workshops for all staff regarding risk management, to raise awareness, provide key information on current requirements and to help achieve buy in at all levels of the organisation;
- The people strategy should be agreed and communicated as soon as possible. This could be supported by the formation of a people group to help drive forward the strategy and provide a focal point for all people related issues; and
- All staff training actually completed should be recorded and monitored so that management are able to fully analyse what Learning & Development is being carried out, what kind of training is being undertaken and where there are issues with individuals not achieving enough Learning & Development.

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

	Total Recs	High	Medium	Low
C1 Risk Register	1		1	
Staffing/Capability	1		1	
Overall	2		2	

4. 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 2; and

EXECUTIVE SUMMARY

- 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 the recommendation have been implemented effectively.

4.3 Management should implement the agreed recommendations before or by the agreed due dates and:

- advise HGIAS that the actions have been completed; and
- provide relevant evidence to demonstrate how the recommendations have been implemented effectively.

4.4 If HGIAS does not receive a response from management by or before the agreed due dates, HGIAS will then follow up all high and medium rated recommendations with the action owner on the relevant due date (as specified in the agreed action plan). This is to verify that the recommendation have been implemented effectively.

4.5 In the absence of a response to our follow up, the outstanding recommendations will be escalated to the relevant Director and routinely reported to the Audit and Governance Committee.

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

4.7 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 action taken to implement the recommendation to take place

№	RATING	RECOMMENDATIONS	MANAGEMENT RESPONSE	AGREED ACTION PLAN: OWNER & PLANNED IMPLEMENTATION DATE	*EXPECTED EVIDENCE TO DEMONSTRATE RECOMMENDATION IMPLEMENTATION
1.	M	The current strategic risk register (for the C1 Capability risk) should be reviewed and updated to ensure it provides more comprehensive data to help inform management decisions on risk, including:			A revised strategic risk register which has addressed all of the recommendations and has been reviewed and signed off by management. CMG risk meeting minutes reflecting the discussion.
		• Review all current mitigating actions to ensure they include effective controls which address the root cause of the risk identified and are sufficient to reduce the severity;	Agreed. We already do such a review at every risk CMG, but we could usefully focus more on ensuring the controls are really controls, and are controlling root causes	Next available CMG Risk meeting – February 2018 Paula Robinson & Helen Crutcher	
		• Contingency actions in instances where identified mitigating actions have not been effective should be detailed, or a clear rationale for these not being in place should be included;	This links to a useful point made at AGC in October – which was about considering the adequacy of controls for any over-tolerance risks. This is done, but we could be clearer in the risk commentary if we have chosen to tolerate the position for a period of time, or if no further controls are available.	Next available CMG Risk meeting – February 2018 Paula Robinson & Helen Crutcher	
		• The register should include a risk appetite/tolerance which clearly reflects the amount of risk HFEA is	Agreed and implemented this week,	We have updated this section of the risk policy now, to clarify what we mean by risk appetite and risk tolerance, and to state	

RECOMMENDATIONS TABLE

№	RATING	RECOMMENDATIONS	MANAGEMENT RESPONSE	AGREED ACTION PLAN: OWNER & PLANNED IMPLEMENTATION DATE	*EXPECTED EVIDENCE TO DEMONSTRATE RECOMMENDATION IMPLEMENTATION
		willing to undertake to meet their strategic objectives; • An additional column should be added which details the latest actions carried out by management and confirms that the risk and mitigation has been reviewed and agreed.	Agree that we should find a way of making it clearer what the most recent actions/controls have been. Dates of recent risk reviews appear on the summary page at the start of the risk register.	that our risk appetite is low. We have also reflected this in the risk register. Paula Robinson & Helen Crutcher We will look at this and see if we can achieve the same thing without adding a column (since that would be hard to fit in elegantly). Paula Robinson & Helen Crutcher	
2.	M	HFEA should put in place mechanisms to ensure that information captured through exit interviews and staff surveys to identify the root causes behind staff turnover, is used effectively to implement practical changes to bring turnover levels in line with agreed tolerances. This should include, but not limited to: • Ensuring that all information gathered from staff during exit interviews and staff surveys is reviewed in detail, with an action plan produced to respond positively to the findings. Any actions agreed should have senior management	Agreed. We will look at this suggestion in the near future.	Discussion at next available SMT (before end of 2017). Juliet Tizzard Paula Robinson	A management action plan which provides details of planned actions for addressing the root cause of current staff turnover in HFEA, incorporating some or all of the elements detailed in the recommendation.

RECOMMENDATIONS TABLE

№	RATING	RECOMMENDATIONS	MANAGEMENT RESPONSE	AGREED ACTION PLAN: OWNER & PLANNED IMPLEMENTATION DATE	*EXPECTED EVIDENCE TO DEMONSTRATE RECOMMENDATION IMPLEMENTATION
		sponsorship to ensure there is the requisite accountability and a clear mandate for implementing the actions agreed; • Development of a clear workforce strategy which supports management in the recruitment and retention of staff	Agreed – this is in progress.	Finalisation discussion planned at leadership away day on 29 November 2017. Publication shortly thereafter. Peter Thompson Yvonne Akinmodun	

FINDING/OBSERVATION

1. FINDING/OBSERVATION:
Updating of strategic risk register

RISK RATING: Medium

Boards should use risk management actively as a key driver in achieving value for money and be confident that risks are being managed appropriately. Risk registers are an important tool to support this and ensure that management take decisions based on good quality information without being overly optimistic.

It is therefore important that registers are kept up-to-date and are complete in terms of the information they capture.

We identified a number of issues with the current strategic risk register (for the C1 Capability risk):

- A number of the current mitigations listed are status updates, and do not explicity detail the controls in place to effectively manage or reduce the assocated risk. There is a potential therefore that HFEA are exposed to a greater level of risk, without these controls being identified and in place;
- There were no contingency actions identifed to support the mitigations, which would leave HFEA exposed should the agreed mitigations fail or prove ineffective. Where contingencies are discussed and not deemed appropriate, this should be clearly recorded to show that this has been considered;
- There was no indication on the register regarding HFEA's overall risk tolerance/appetite level. This is an important part of the risk management process, as it allows clearer identification of appropriate mitigations and actions, which would help manage the risk within agreed tolerances; and
- There was no indication regarding the latest actions carried out by management against any of the risks, and it is unclear what action has been taken, by whom and what impact this had on the risk.

RISK/IMPLICATION:

That HFEA are not effectively managing the capability risk within agreed tolerances, and that any mitigations and contingencies are not effective in managing or reducing the risk.

RECOMMENDATION:

The current strategic risk register (for the C1 Capability risk) should be reviewed and updated to ensure it provides more comprehensive data to help inform management decisions on risk, including:

- Review all current mitigating actions to ensure they include effective controls which address the root cause of the risk identified and are sufficient to reduce the severity;
- Contingency actions in instances where identified mitigating actions have not been effective should be detailed, or a clear rationale for these not being in place;
- The register should include a risk appetite/tolerance which clearly reflects the amount of risk HFEA is willing to undertake to meet their strategic objectives; and
- An additional column should be added which details the latest actions carried out by management and confirms that the risk and mitigation has been reviewed and agreed.

FINDING/OBSERVATION

2. FINDING/OBSERVATION: **Staffing Levels**
RISK RATING: Medium
We identified that at the time of the audit staff turnover within HFEA was increasing (the latest documented figure was 33% per annum) and that this percentage was above the 15% key performance indicator set by HFEA. Performance indicators are in place and monitored, supported by detailed management information. There was also evidence of work by HFEA to identify the root causes behind the high turnover levels, such as exit interviews, staff surveys and task and finish groups. However, we could not see evidence of any clear processes in place to effectively use the information gathered, and implement actions to help manage and ultimately reduce this risk.
RISK/IMPLICATION:
There is the potential that HFEA are exposed to continued high staff turnover, loss of experience and expertise, which could lead to knowledge gaps and disruption to key areas of the business, affecting the service provided.
RECOMMENDATION:
HFEA should put in place mechanisms to ensure that information captured through exit interviews and staff surveys to identify the root causes behind staff turnover, is used effectively to implement practical changes to bring turnover levels in line with agreed tolerances. This should include, but not limited to: • Ensuring that all information gathered from staff during exit interviews and staff surveys is reviewed in detail, with an action plan produced to respond positively to the findings. Any actions agreed should have senior management sponsorship to ensure there is the requisite accountability and a clear mandate for implementing the actions agreed; and • Development of a clear workforce strategy which supports management in the recruitment and retention of staff.

Suggested 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.

SUMMARY OF AUDIT RECOMMENDATIONS

Year of Rec.	Category	Audit	Section	Rec #	Recommendations	Action Manager	Proposed Completion Date	Complete this cycle?
2017/18	M	DH Internal Audit	Data Loss	1	**Clinic governance oversight**	*Chris Hall, Senior Inspector (Information)*	*Post April 2018*	No
	M			2	**Policy Review**	*Dan Howard, CIO*	*May 2018*	No
	M			3	**Staff Training**	***TBC** (Dan Howard, CIO & Head of HR)*	*December 2017*	No
	M			4	**Business Continuity Testing**	*Dan Howard, CIO*	*November 2017*	Yes
	M		Risk Management	1	**Risk Register**	*Paula Robinson, Head of Planning & Governance*	*February 2018*	No
	M			2	**Staffing / Capability**	*Paula Robinson, Head of Planning & Governance*	***TBC***	No
TOTAL	**6**							

FINDING/*RISK*	Recommendation	Management Response and agreed actions / Progress update	Owner/Completion date
2017/18 – INTERNAL AUDIT CYCLE			
DATA LOSS			
1. Clinic governance oversight			
The HFEA regularly inspects UK fertility clinics and research centres. This ensures that every licensed clinic or centre is adhering to standard safety. The purpose of an inspection is to assess a clinic's compliance with the Human Fertilisation and Embryology Act 1990 (as amended), licence conditions; General Directions and the provisions of the Code of Practice. The results of these audits from 2016/17 have not identified any significant weaknesses. The NAO accompany one visit per year.	The new Senior Inspector role should include responsibility over the Clinics' governance arrangements in managing data loss, including: a. Clinics' information governance arrangements to mitigate the risk of data losses; b. Clinics' arrangements for staff training on information management; c. Clinics' BCP arrangements.	**The Senior Inspector (Information) role has been reviewed and it includes responsibilities for reviewing Information Governance. This includes staff training and security arrangements which includes reviewing BCP planning.** ***Inspection regime to be updated to reflect requirements within the new Senior Inspector (Information) post – April 2018*** ***Nov 17 update:*** *no update*	***Chris Hall, Senior Inspector (Information)*** ***Post April 2018***
2. Policy Review			
Key policies and some of the Standing Operating Procedures were not up to date and were not reviewed on a regular basis - there is a risk that the policy may be out of date and result in incorrect processes being followed.	Key data and information policies should be reviewed periodically to ensure that they are current and aligned.	**Information Access Policy and SOPs to be reviewed, updated and ratified to reflect GDPR requirements. Staff Security Procedures (Acceptable Use Policy) to also be updated** ***To align with GDPR legislation and to be updated as a component of the HFEA GDPR Action Plan - May 2018. Update and approve at CMG – January 2018*** ***Nov 17 update:*** *We have established a joint project with the HTA and we are developing an overarching project plan and have started the assessment against the 'Nymity Data Privacy Accountability Scorecard'. The recruitment to the IG Project Officer is ongoing.*	***Owner: Dan Howard, CIO*** **May 2018**

3.	**Staff Training**			
We identified that the HFEA Business Continuity Plan has not been tested on a regular basis. It was therefore not possible for HFEA to provide assurance that the BCP remains current, fit for purpose and reflects key personnel change to ensure roles and responsibilities are clear.	A process should be put in place to ensure that HFEA are able to capture and monitor all mandatory information management learning and development carried out.	**We will refresh our approach to the completion of the following modules of mandatory training in IG. Our target is that all staff will have completed these in the previous 12 months by the end of the calendar year. The modules are:** • **Responsible for information: general user;** • **Responsible for information: information asset owner (IAOs to complete); and** • **Responsible for information: senior information risk owner (SIRO to complete)** ***All staff – December 2017. The framework for mandatory training (in all areas including information training requires refresh). In any event whilst many staff have undertaken training within 12 months we will use Oct-Dec period to ensure all staff have completed, with sign off from Managers.*** ***Nov 17 update:*** *Information management training has been identified for all staff. Information Asset Owners, SIRO and all remaining staff will be expected to complete this before the end of December 2017.*	***Dan Howard, CIO*** *(Yvonne Akinmodun)* **December 2017**
4.	**Business Continuity Testing.**			
There was no management assurance documented to demonstrate that all HFEA staff have complete the mandatory e-learning 'responsible for information' training. Therefore, there is a risk that this training has not been carried out by some or all staff resulting in staff handling data incorrectly potentially leading to loss of data.	The BCP should be updated on a regular basis to ensure that it reflects all key changes and is appropriately tested to ensure that it is fit for purpose.	**BCP test and table top test to take place in September 2017. BCP to be updated to reflect lessons learnt from the above tests and to reflect new CIO role responsible.** ***BCP summary test findings report submitted to AGC in October 17. BCP approved by CMG in November 17.*** ***Nov 17 update:*** *BCP summary findings presented to AGC in October - action complete. The revised BCP has been circulated and will be reviewed at CMG on 23 November 2017.* ***Recommendation completed.***	***Dan Howard, CIO*** **November 2017** **COMPLETE**

RISK MANAGEMENT				
5.	**C1 Risk Register**			
Updating of strategic risk register That HFEA are not effectively managing the capability risk within agreed tolerances, and that any mitigations and contingencies are not effective in managing or reducing the risk.	The current strategic risk register (for the C1 Capability risk) should be reviewed and updated to ensure it provides more comprehensive data to help inform management decisions on risk, including: • Review all current mitigating actions to ensure they include effective controls which address the root cause of the risk identified and are sufficient to reduce the severity; • Contingency actions in instances where identified mitigating actions have not been effective should be detailed, or a clear rationale for these not being in place should be included; • The register should include a risk appetite/tolerance which clearly reflects the amount of risk HFEA is willing to undertake to meet their strategic objectives; and • An additional column should be added which details the latest actions carried out by management and confirms that the risk and mitigation has been reviewed and agreed.	***A revised strategic risk register which has addressed all of the recommendations and has been reviewed and signed off by management.*** ***Agreed. We already do such a review at every risk CMG but we could usefully focus more on ensuring the controls are really controls and are controlling root causes. Next available CMG Risk meeting*** ***This links to a useful point made at AGC in October – which was about considering the adequacy of controls for any over-tolerance risks. This is done but we could be clearer in the risk commentary if we have chosen to tolerate the position for a period of time, or if no further controls are available. Next available CMG Risk meeting*** ***Agreed and implemented. We have updated this section of the risk policy now, to clarify what we mean by risk appetite and risk tolerance, and to state that our risk appetite is low. We have also reflected this in the risk register.*** ***Agree that we should find a way of making it clearer what the most recent actions/controls have been. Dates of recent risk reviews appear on the summary page at the start of the risk register.*** ***We will look at this and see if we can achieve the same thing without adding a column (since that would be hard to fit in elegantly).***	***Owner: Paula Robinson, Head of Planning and Governance*** ***Helen Crutcher*** ***February 2018*** ***February 2018*** ***Completed*** ***TBC***

6.	Staffing / Capability		
There is the potential that HFEA are exposed to continued high staff turnover, loss of experience and expertise, which could lead to knowledge gaps and disruption to key areas of the business, affecting the service provided.	HFEA should put in place mechanisms to ensure that information captured through exit interviews and staff surveys to identify the root causes behind staff turnover, is used effectively to implement practical changes to bring turnover levels in line with agreed tolerances. This should include, but not limited to: • Ensuring that all information gathered from staff during exit interviews and staff surveys is reviewed in detail, with an action plan produced to respond positively to the findings. Any actions agreed should have senior management sponsorship to ensure there is the requisite accountability and a clear mandate for implementing the actions agreed; and • Development of a clear workforce strategy which supports management in the recruitment and retention of staff.	***A management action plan which provides details of planned actions for addressing the root cause of current staff turnover in HFEA, incorporating some or all of the elements detailed in the recommendation.*** ***Agreed. We will look at this suggestion in the near future. Discussion at the next available SMT.*** ***Agreed – this is in progress. Finalisation discussion planned at leadership and away day on 29 November 2017. Publication shortly thereafter.***	***Juliet Tizzard, Director of Strategy & Corporate Affairs*** ***Paula Robinson*** ***Before end of 2017*** ***Peter Thompson, CEO*** ***Yvonne Akinmodun*** ***TBC***

Digital Programme Update: including data submission

Strategic delivery:	☒ Setting standards	☐ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item	7		
Paper number	AGC (05/12/2017) 579 DH		
Meeting date	05 December 2017		
Author	Dan Howard, Chief Information Officer		
Output:			
For information or decision?	For information		
Recommendation	The Committee is asked to note: • The progress update on data migration and the submission system • The update relating to launch dates and availability, and transitional arrangements.		
Resource implications	None		
Implementation date	During 2017–18 and 2018 - 19 business year		
Communication(s)	Regular, range of mechanisms		
Organisational risk	☐ Low	☒ Medium	☐ High
Annexes:	None		

1. Background

1.1. On the closure of the formal IfQ programme, it was agreed that progress on the residual work should be reported to Audit and Governance Committee.

1.2. In October 2017, AGC received an update on treatment data submission system. This paper provides an update on progress and includes an overview of the follow-on transitional arrangements which will be undertaken once these elements have been completed.

2. Introduction

2.1. The Committee had some concerns as to the clarity provided at its last meeting regarding progress against expected milestones, particularly in relation to data migration work. Significant progress has since been made in terms of planning and further scoping and this was reported to the Authority meeting in November.

2.2. The data submission system itself is progressing well and we are pleased to report that significant parts of the new system are now ready. We have launched our APIs (Application Program Interface) and started dialogue with system suppliers. The APIs are the technical system linkages which mean that third party IT systems can 'talk' directly to our register allowing data to be provided in the structured format we require after applying the validation rules we have set. Use of new validation rules will ensure the highest quality data is received from clinics – reducing our 'checking' overhead.

2.3. Further to data migration and completion of the data submission system, we expect to launch at the end of April 2018. It is important to note that those clinics using a third-party system will require their system suppliers to ensure their systems are compliant with our new dataset. Those 'transitional arrangements' are now a focus of our work.

3. Data Migration

3.1. We appointed an experienced project manager to undertake a root and branch review of the data migration work and ensure appropriate management oversight and controls are in place. The review confirmed:

- The overall Project Plan that is in place provides clarity of the tasks required to complete development and testing of the data migration processes by end March 2018, with follow on assurance processes during April 2018 consistent with the completion of the Register information submission system.
- Tasks have been allocated and are being actively managed across the team using the 'TFS' system which chases up and reports exceptions
- Project controls are in place with weekly review sessions and bi-weekly planning sessions

- There is a bi-weekly progress report, with weekly exception reports where required, to the CIO and Director of Compliance and Information.

3.2. The project consists of a number of deliverables to develop and test the migration process ahead of the final migration. These have been split into discrete areas, with each following a similar process:

- Producing extracts from the legacy database
- Validating the extract is complete and ensuring integrity and consistency of the data
- Loading the extract into the new database and testing it retains integrity and consistency

3.3. Alongside this work we must also fulfil our commitments within our extant IT strategy – to reduce our reliance on 'on-premise' infrastructure, that is the physical servers based in Spring Gardens, and move to Microsoft UK data centres. In line with the strategy this delivers greater assurance relating to data security and resilience.

3.4. There remain risks within the project, mainly concerning

- critical local knowledge of the data and data base which resides in a few key individuals.
- risks relating to the duration of remedial work given that this cannot be predicted
- resourcing risks – availability of specialist skills.

3.5. These risks are being mitigated as far as possible and need careful monitoring and management. We are confident that effective management oversight and project controls, outlined above, are in place. Some additional back-fill resource has now also been allocated to the project.

3.6. Summary information from the Project Plan is available here.

Deliverable	Start date	Due date	Status
Data Migration Process Development:			Complete
Data Migration Process Development: DI Cycles			Complete
Data Migration Process Development: IVF Cycles / Billing	19/10/17	17/01/18	In Progress
Data Migration Process Development: Early Outcome/Outcome	19/10/17	15/11/17	Complete
Data Migration Process Development: Image Storage	02/12/17	15/12/17	
TRIAL LOAD 4	17/01/18		
Data Migration Process Development: Linkages	18/01/18	14/02/18	
Data Migration Process Development: Gamete Movement	15/02/18	14/03/18	
PRE-LIVE TRIAL LOAD	15/03/18	28/03/18	
Third party (Northdoor) Assurance Audit	29/03/18	18/04/18	
READY FOR GO-LIVE	30/04/18		

4. Data Submission System

4.1. Significant progress has been made and several modules have now been completed including patient, partner, donor, surrogate and intended parent registrations.

4.2. We have started the process of exposing EPRS (Electronic Patient Record System Providers) to our APIs for modules completed to date. This work is progressing well and we are delighted that feedback from them has been very positive so far.

4.3. The next stage of EPRS engagement includes releasing the APIs for Donor Insemination (DI) Cycles, Early Outcome (EO), Pregnancy Outcome (PO). We plan that these will be completed and released to providers during the week commencing 04 December 2017.

4.4. Development relating to IVF is expected to be completed in January 2018. This is one of the largest components of the system to be developed.

5. Transitional Arrangements

5.1. The project work above provides us with a new submission system and Register, with the functionality we require to collect and store high quality data. Both we and the clinics we regulate will see a significant improvement when these systems go live. The arrangements we put in place for all clinics are being finalised - in particular our plan for ongoing engagement with clinics and suppliers of third party systems.

5.2. The first clinics using the new system will be those using the current HFEA ‘EDI’ system – to use the new data submission system. The suppliers of third party systems to clinics will need time to implement the upgrades required to comply with our new dataset. The clinics

will also need time to adapt. We have only recently released initial APIs to suppliers and the feedback to date is positive. That said, we are sensitive to clinics and their suppliers about how long it will take for them to complete the upgrades. Many will wish to proceed quickly, some will need more time. Further to more engagement we will be issuing a deadline for suppliers to have completed their upgrades and to be compliant with our requirements, after which all clinics will need to use our system or via a compliant third-party system.

6. Recommendation

The Committee is asked to note:

- The progress update on data migration and the submission system
- The update relating to launch dates and availability, and transitional arrangements.

Resilience, Business Continuity Management and Cyber Security

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

1. Background

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

2. Progress update

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

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

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

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

3. Recommendation

The Committee is asked to note:

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

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 (05/12/2017) 581 HC]		
Meeting date	5 December 2017		
Author	Helen Crutcher, Risk and Business Planning Manager		
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 received the risk register at its meeting on 15 November.

1.2. CMG reviewed the risk register at its meeting on 22 November. CMG reviewed all risks, controls and scores.

1.3. CMG and Authority's comments are summarised at the end of the risk register, which is attached at Annex A. The annex also includes a graphical overview of residual risk scores plotted against risk tolerances.

1.4. One of the seven risks is currently above tolerance.

Additions to the register

1.5. AGC should note that we have now added statements on risk tolerance and appetite in the background information of the report. This sets out our general position in relation to addressing the tolerance levels of particular risks.

1.6. We have also been reviewing the risk policy in the light of previous AGC and initial feedback from an advisory internal audit report, which is currently being finalised. The policy will reflect the statements on risk appetite and tolerance and it will clearly set out our approach for dealing with over-tolerance risks. This is partly about reviewing the adequacy of mitigations but also about clearly explaining the rationale if there are periods when we may be unable to bring a risk down to our desired tolerance level.

1.7. The revised policy will be discussed and agreed at the Corporate Management Group meeting in February. We will relaunch the policy following agreement.

2. Recommendation

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

Latest review date – 22/11/2017

Strategic risk register 2017/18

Risk summary: high to low residual risks

Risk area	Strategy link*	Residual risk	Status	Trend**
C1: Capability	Generic risk – whole strategy	**16 – High**	Above tolerance	⇧⇔⇔⇔
LC1: Legal challenge	Generic risk – whole strategy	**12 – High**	At tolerance	⇩⇔⇔⇔
OC1: Organisational change	Generic risk – whole strategy	**9 – Medium**	At tolerance	⇔⇔⇩⇔
FV1: Financial viability	Generic risk – whole strategy	**9 – Medium**	At tolerance	⇔⇔⇔⇔
CS1: Cyber security	Generic risk – whole strategy	**6 – Medium**	At tolerance	⇔⇔⇔⇔
RE1: Regulatory effectiveness	Improving standards through intelligence	**6 – Medium**	At tolerance	⇔⇔⇔⇔
ME1: Effective communications	Safe, ethical effective treatment Consistent outcomes and support	**6 – Medium**	At tolerance	⇔⇔⇔⇔

* Strategic objectives 2017-2020:

Safe, ethical effective treatment: Ensure that all clinics provide consistently high quality and safe treatment

Safe, ethical effective treatment: Publish clear information so that patients understand treatments and treatment add ons and feel prepared

Safe, ethical effective treatment: Engender high quality research and responsible innovation in clinics

Consistent outcomes and support: Improve access to treatment

Consistent outcomes and support: Increase consistency in treatment standards, outcomes, value for money and support for donors and patients

Improving standards through intelligence: use our data and feedback from patients to provide a sharper focus in our regulatory work and improve the information we produce

** This column tracks the four most recent reviews by AGC, CMG, or the Authority (eg,⇧⇔⇩⇔). Recent review points are:

Risk register 2017-2020: CMG 6 September ⇨ AGC 3 October ⇨ Authority 15 November ⇨ CMG 22 November

FV1: There is a risk that the HFEA has insufficient financial resources to fund its regulatory activity and strategic aims.

Inherent risk level:			Residual risk level:		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	4	16 - High	**3**	**3**	**9 - Medium**
Tolerance threshold:					**9 - Medium**

Risk area	Risk owner	Links to which strategic objectives?	Trend
Financial viability FV1: Income and expenditure	Richard Sydee, Director of Finance and Resources	Whole strategy	⇔⇔⇔⇔

Commentary
At tolerance. As of Q2, we are showing a surplus against budget which is due to the steady increase in our treatment fee income and the slow expenditure activity of which unfilled vacancies are a major part. Our forecast for the year is likely to be a surplus subject to any new legal issues and assuming spend on the data submission and migration projects is maintained. The work that is currently in progress to produce a model for forecasting treatment fee income may mean that the residual risk will be able to be reduced, but this will not be clear until the model is finalised and agreed by the Authority in early 2018. A paper will go the Authority in January. A deep-dive review of this risk is planned in the light of the outcomes of this and this will be reflected in the next update to AGC in March.

Causes / sources	Mitigations	Timescale / owner
Our annual income can vary significantly as: - Our income is linked directly to level of treatment activity in licensed establishments - Forecasting treatment numbers is complex - We rely on our data submission system to notify us of billable cycles.	Activity levels are tracked and significant changes are discussed at CMG, who would consider what work to deprioritise and reduce expenditure.	Monthly (on-going) – Richard Sydee
	Fees Group enables dialogue with sector about appropriate fee levels.	Ongoing – Richard Sydee
	We have sufficient reserves to function normally for a period if there was a steep drop-off in activity, or clinics were not able to submit data and could not be invoiced. If this happened, resolving it would be high priority, and the roll-out of the new data submission system will be planned carefully.	In place – Richard Sydee/Nick Jones
	Work on the drivers of treatment fees to better understand the likely future trends in treatment cycle activity.	Begun in Q2. Ongoing – Richard Sydee

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
Project scope creep.	Senior Finance staff present at Programme Board. Periodic review of actual and budgeted spend by Digital Projects Board (formerly IfQ) and monthly budget meetings with finance.	Ongoing – Richard Sydee or Morounke Akingbola
	Cash flow forecast updated.	Monthly (on-going) – Morounke Akingbola
Risk interdependencies (ALBs / DH)	**Control arrangements**	**Owner**
DH: Legal costs materially exceed annual budget because 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
DH: 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

C1: There is a risk that the HFEA experiences unforeseen knowledge and capability gaps, threatening delivery of the strategy.

Inherent risk level:			Residual risk level:		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
5	4	20 – Very high	**4**	**4**	**16 - High**
Tolerance threshold:					**12 - High**

Risk area	Risk owner	Links to which strategic objectives?	Trend
Capability C1: Knowledge and capability	Peter Thompson, Chief Executive	Whole strategy	⇧⇔⇔⇔

Commentary

Above tolerance.

This risk and the controls are focused on business as usual capability, rather than capacity, though there are obviously some linkages between capability and capacity.

Since we are a small organisation, with little intrinsic resilience, it seems prudent to retain a low tolerance level. We are currently in a period of turnover and internal churn, with some knowledge gaps, and data submission and migration work ongoing. As a result, the tolerance level for this risk was raised from 6 to 12 at CMG in May. And in September, CMG raised the risk level in recognition of the additional impact of organisational change.

Action plan

Heads and managers are proactively treating this risk by ensuring that handovers are as full and thorough as possible and ensuring that recruitment happens as quickly as possible. Our Interim Head of HR, Yvonne Akinmodun, has been working on the new people strategy and this was discussed with Heads and SMT at a leadership away day in November.

Alongside this, an improved system for formalised knowledge capture and handover is being scoped. A formalised corporate process should go further to ensuring that all staff know what is required and that handovers are of a high quality. These further actions should help to mitigate this risk and bring it back within tolerance, although these are not yet fully in place. We should be able to reassess the effectiveness of these mitigations in early 2018.

Causes / sources	Mitigations	Timescale / owner
High turnover, sick leave etc., leading to temporary knowledge loss and capability gaps.	Staff have access to Civil Service Learning (CSL); expectation is five working days per year of learning and development for each member of staff. Staff are encouraged to identify personal development opportunities with their manager, through the PDP process, making good use of CSL.	In place – Yvonne Akinmodun (Interim Head of HR)/Peter Thompson

	Organisational knowledge captured via documentation, handovers and induction notes, and manager engagement.	In place – Yvonne Akinmodun
	Vacancies are addressed speedily, and any needed changes to ways of working or backfill arrangements receive immediate attention.	In place – Peter Thompson
Poor morale leading to decreased effectiveness and performance failures.	Engagement with the issue by managers through team and one-to-one meetings to obtain feedback and identify actions to be taken.	In place – Peter Thompson
	Implementation of staff survey outcomes, followed up after December 2016 staff conference (follow-up staff conference held on 10 July 2017). Task and Finish Groups submitted ideas for improvements, which are being included in the people strategy for 2017-2020.	Survey and staff conferences 2016 done – Rachel Hopkins Follow-up plan and communications in place – Peter Thompson
Particular staff changes could lead to specific 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
Insufficient Register team resource to deal properly with OTR enquiries.	The team is now at full capacity (headcount) and this risk is reducing over time as the new member of staff gets up to speed.	In place – Nick Jones
Increased workload either because work takes longer than expected or reactive diversions arise.	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
	Oversight of projects by both Programme Board and CMG, to ensure that projects end through due process (or closed, if necessary).	In place – Paula Robinson
	Learning from Agile methodology to ensure we always have a clear ‘definition of done’ in place, and that we record when products/outputs have met the ‘done’ criteria and are deemed complete.	Partially in place – agile approach to be brought into project processes under new project governance framework – by early 2018/19

		Paula Robinson
	Early emphasis on team-level service delivery planning for the next business year, with active involvement of team members. CMG will continue to review planning and delivery.	In place – Paula Robinson
	Planning and prioritising data submission project delivery, and therefore strategy delivery, within our limited resources.	In place until project ends in Spring 2018 – Paula Robinson
Possible future increase in capacity and capability needed to process mitochondrial donation applications.	Starting to be considered now, but will not be known for sure until later, so no controls can yet be put in place. Only one clinic licensed to provide these treatments, applications unlikely to be many at first. New licensing processes for mitochondrial donation are in place (decision trees etc). One Licence Committee variation agreed, and the first Statutory Approvals Committee decision was at August 2017 meeting. As at November three patient applications had been considered.	Issue for further consideration – Director of Strategy and Corporate Affairs
Technical issues with our communications systems since our office move in 2016. This leads to poor service (missed calls, poor quality Skype meetings), reputational impacts, additional costs (meetings having to be held externally), and potentially to complaints.	The IT team has been working to identify and resolve the issues, with staff encouraged to continue to send support tickets. In summer 2017 an external expert was commissioned to assist and the system subsequently displayed improvements, although a number of issues have continued to affect the system and so a new company is now sought for further review and assurance. Continued use of external venues with appropriate facilities. As of November 2017, the switchboard has been replaced. This may prevent some of the Skype issues that have been reported, though we will monitor the effectiveness of this over the coming months.	In progress – Nick Jones Since he started in Sept 2017, Dan Howard, the CIO has been monitoring these issues and focussing on ensuring effective controls.
Risk interdependencies (ALBs / DH)	**Control arrangements**	**Owner**
Government/DH: 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.	We were proactive in reducing headcount and other costs to minimal levels over a number of years. We have also been reviewed extensively (including the McCracken review and Triennial Review).	In place – Peter Thompson

OC1: There is a risk that the implementation of organisational changes results in instability, loss of capability and capacity, and delays in the delivery of the strategy.

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	4	16 – High	**3**	**3**	**9 - Medium**
Tolerance threshold:					**9 - Medium**

Risk area	**Risk owner**	**Links to which strategic objectives?**	**Trend**
Organisational change OC1: Change-related instability	Peter Thompson, Chief Executive	Whole strategy	⇔⇔⇩⇔

Commentary
At tolerance. For some months, this risk was above tolerance and its impact was closely related to the C1, Capability risk. In November, with the agreement of the Authority, this risk was reduced back to tolerance. This was done in the light of the fact that almost all the agreed voluntary redundancies had taken place and most of the recruitment is complete. The Authority also agreed that this strategic risk could be removed at the end of the business year, at which point all of the planned voluntary redundancies will have taken place along with most of the remaining recruitment. Any outstanding risk sources would be considered at that time, to ensure that they are captured in the relevant operational risk logs or under the Capability strategic risk, as relevant.

Causes / sources	**Mitigations**	**Timescale / owner**
The change period may lead to dips in morale, commitment, discretionary effort and goodwill. 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.	Clear published process, with documentation.	In place – Peter Thompson
	Consultation, discussion and communication, with opportunity to comment, and being responsive and empathetic about staff concerns. Staff informed of likely developments and next steps and, when applicable, of personal role impacts and choices.	Completed – Peter Thompson
	Relatively short timeline for decision making, so that uncertainty does not linger.	In place – Peter Thompson
	HR policies and processes are in place to enable us to manage any individual situations that arise.	In place – Yvonne Akinmodun

	Employee assistance programme (EAP) support accessible by all.	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).	Policies and processes to ensure we treat staff fairly and consistently, particularly those '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 – Yvonne Akinmodun
	Good decision-making and risk management mechanisms in place. Knowledge retention via good records management practice, SOPs and documentation.	In place – Peter Thompson
Potential impact on our ability to complete IfQ on time.	Ability to use more contract staff if need be.	In place – Peter Thompson
Implementing the new structure involves significant additional work across several teams to embed it so that the benefits are realised. There will also be result in some internal churn.	Business plan discussions acknowledging that work in teams doing IfQ or organisational change should not be overloaded.	In place – Paula Robinson
	CMG able to change priorities or timescales if necessary, to ensure that change is managed well.	In place – Paula Robinson
	Organisational development activity will continue, including summer awayday (10 July 2017), to support new ways of working development. A leadership awayday (November 2017) and another all staff awayday will happen in January 2018.	In place for 2017 and planned for 2018 – Yvonne Akinmodun
Additional pressure on SMT, HR and Heads, arising from the need to manage different impacts 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
Level of service to Authority members may suffer while the changes are implemented,	Communicate the changes clearly to Authority members so that they understand when staff are particularly under pressure, and that they will have	In place, with some implementation

negatively impacting on the relationship between staff and members.	reduced capacity. Inform Members when staff are new in post, to understand that those staff need the opportunity to learn and to get up to speed.	ongoing – Peter Thompson
Once the changes have been implemented, a number of staff will simultaneously be new in post. This carries a higher than normal risk of internal incidents and timeline slippages while people learn and teams adapt.	Recognition that a settling in period where staff are inducted and learn, and teams develop new ways of working is necessary. Formal training and development provided where required. Knowledge management via records management and documentation.	To be implemented, Yvonne Akinmodun will review onboarding methods – Peter Thompson
Bedding down the new structure will necessarily involve some team building time, developing new processes, staff away days to discuss new ways of working, etc. This will be challenging given small organisational capacity and ongoing delivery of business as usual.	Change management will be prioritised, where possible, 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.	Development day planned in November – Yvonne Akinmodun
The new model may not achieve the desired benefits, or transition to the new model could take too long, with staff losing faith in the model.	The model will be kept under review following implementation to ensure it yields the intended benefits.	A review of the new model will be presented to the Authority in May 2018 – Peter Thompson
Risk interdependencies (ALBs / DH)	**Control arrangements**	**Owner**
-		

CS1: There is a risk that the HFEA has unsuspected system vulnerabilities that could be exploited, jeopardising sensitive information and involving significant cost to resolve.

Inherent risk level:			Residual risk level:		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
5	4	20 – Very high	**3**	**2**	**6 - Medium**
Tolerance threshold:					**6 - Medium**

Risk area	Risk owner	Links to which strategic objectives?	Trend
Cyber security CS1: Security and infrastructure weaknesses	Nick Jones, Director of Compliance and Information	Whole strategy	⇔⇔⇔⇔

Commentary
At tolerance. The cyber-security event earlier in 2017, affecting the NHS and other organisations demonstrates that there is no room for complacency. However recent audits and our own assessments indicate that the HFEA is well protected. We were not affected by the 2017 incident.

Causes / sources	Mitigations	Timescale / owner
Insufficient governance or board oversight of cyber security risks (relating to awareness of exposure, capability and resource, independent review and testing, incident preparedness, external linkages to learn from others).	AGC receives regular information on cyber-security and associated internal audit reports. Internal audit report (2017) gave a 'moderate' rating, and recommendations are being actioned. Detailed information on our security arrangements is available in other documents. A business continuity plan is in place.	In place - Nick Jones/Dan Howard
Recent system infrastructure changes open up potential attack surfaces or new vulnerabilities. Our relationship with clinics is now more digital than ever before, and patient data or clinic information could therefore be exposed to attack.	All key IfQ products were subject to external expert advice and penetration testing, with recommendations implemented.	In place - Nick Jones/Dan Howard
	A security consultant provided advice throughout IfQ. At the end of the programme, we have received documented assurance of security and the steps necessary to maintain that security at a high level. Penetration testing for the portal and website (completed and passed).	In place – Dan Howard

	Ongoing security advice is in place for the development of the new data submission systems.	
We could become more dependent on external advice and support, with the risk that we cannot identify or fix problems quickly.	Budget available to commission external support when needed.	In place – Nick Jones
Confidentiality breach of Register data.	Staff have annual compulsory security training to guard against accidental loss of data or breaches of confidentiality. We know we need to refresh this obligation. Secure working arrangements for Register team, including when working at home.	In place, but corporate oversight of completion of security training is being reviewed – Peter Thompson
Loss of Register or other data by staff or through lack of encryption.	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. CIO will review these arrangements and can do so alongside a review of the arrangements for implementing the new GDPR requirements.	In place – Dan Howard
Register or other data (electronic or paper) becomes corrupted or lost.	Back-ups and warehouse in place to ensure data cannot be lost. Regular monitoring takes place to ensure our data backup regime and controls are effective. Staff have annual compulsory security training to guard against accidental loss of data or breaches of confidentiality.	In place – Nick Jones In place, but the corporate system for oversight is being reviewed by Dec 2017 – Dan Howard/Nick Jones
Infrastructure turns out to be insecure, or we lose connection and cannot access our data.	IT strategy agreed, including a thorough investigation prior to the move to the Cloud, with security and reliability factors considered.	In place – Dan Howard
	Deliberate internal damage to infrastructure, or data, is controlled for through off-site back-ups and the fact that any malicious tampering would be a criminal act.	In place – Nick Jones
Business continuity issue (whether caused by cyber-attack or an event affecting access to Spring Gardens).	Business continuity plan and staff site in place. Improved testing of the BCP information cascade to all staff was undertaken in September 2017 as well as a tabletop test and testing with Authority members.	In place and ongoing – Nick Jones Update done Dave Moysen

	New technology options need to be further explored, to enable us to restore critical on premise systems into a cloud environment if our premises become unavailable for a period. Records management systems to be reviewed in 2017/18. During an outage, staff cannot access TRIM, our current records management system. As above, we need to consider this in relation to GDPR project.	(former Head of IT) – September 2016 A revised BCP was considered by CMG in November and will be finalised shortly – Dan Howard
Poor records management or failure of the document management system.	A comprehensive review of our records management practices and document management system (TRIM) will be conducted in 2018/19, following planned organisational changes and the conclusion of IfQ.	To follow in 2018/19 business year – Peter Thompson
Cloud-related risks.	Detailed controls set out in 2017 internal audit report on this area. We have in place remote access for users, appropriate security controls, supply chain security measures, appropriate terms and conditions with Microsoft Azure, Microsoft ISO 27018 certification for cloud privacy, GCloud certification compliance by Azure, a permission matrix and password policy, a web configuration limiting the service to 20 requests at any one time, good physical and logical security in Azure, good back-up options for SQL databases on Azure, and other measures.	In place – Nick Jones
Risk interdependencies (ALBs / DH)	**Control arrangements**	**Owner**
None. Cyber-security is an 'in-common' risk across the Department and its ALBs.		

LC1: There is a risk that the HFEA is legally challenged in such a way that resources are significantly diverted from strategic delivery.

Inherent risk level:			Residual risk level:		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
5	5	25 – Very high	**3**	**4**	**12 - High**
Tolerance threshold:					**12 - High**

Risk area	Risk owner	Links to which strategic objectives?	Trend
Legal challenge LC 1: Resource diversion	Peter Thompson, Chief Executive	Safe, ethical effective treatment: Ensure that all clinics provide consistently high quality and safe treatment	⇩⇔⇔⇔

Commentary
At tolerance. The judgment on consent to legal parenthood in 2015 and subsequent cases, which include cases where errors have been made as recently as 2016/17, have administrative and policy consequences for the HFEA, and potentially reputational consequences too if we are criticised in judgments. The number of new and upcoming cases has reduced, however, recent cases suggest that learning has not been embedded in every clinic. This raises the question of whether further guidance or training is required in clinics. The most recent judgment is somewhat critical of how the HFEA chose to address certain issues and the guidance it provided to clinics. A judicial review hearing of one discrete element of the IfQ CaFC project was held in December 2016 and January 2017. The HFEA won this case. A decision by the Court of Appeal on whether permission to appeal will be granted is still awaited. This is entirely in the hands of the Court as far as timescales go. A licensing matter was considered by the Appeals Committee in October. The matter was settled by way of consent and having disposed of the appeal the judicial review claim which had been launched concurrently with the appeal became redundant and will be withdrawn. Following the consent order, the executive will be undertaking a piece of work looking at options for the regulation and inspection of groups of clinics.

Causes / sources	Mitigations	Timescale / owner
Assisted reproduction is complex and controversial and the Act and regulations are not beyond interpretation, leading to a need for court decisions.	Panel of legal advisors at our disposal for advice, as well as in-house Head of Legal.	In place – Peter Thompson
	Evidence-based and transparent policy-making and horizon scanning processes.	In place – Hannah Verdin

	Case by case decisions regarding what to argue in court cases, so as to clarify the position.	In place – Peter Thompson
Decisions or our decision-making processes may be contested. Policy changes may also be used as a basis for challenge (Licensing appeals and/or JRs). Note: New guide to licensing and inspection rating on CaFC may mean that more clinics make representations against licensing decisions.	Panel of legal advisors in place, as above.	In place – Peter Thompson
	Maintaining, keeping up to date and publishing licensing SOPs, committee decision trees etc. to ensure we take decisions well. Consistent decision making at licence committees supported by effective tools for committees. Standard licensing pack distributed to members/advisers (refreshed in April 2015).	In place, further work underway on licensing SOPs – Paula Robinson
	Well-evidenced recommendations in inspection reports.	In place – Sharon Fensome-Rimmer
Moving to a bolder strategic stance, eg on add ons or value for money, could result in claims that we are adversely affecting some clinics' business model or acting beyond our powers. Any changes could be perceived as a threat – not necessarily ultimately resulting in legal action, but still entailing diversion of effort.	Risks considered whenever a new approach or policy is being developed. Business impact target assessments carried out whenever a regulatory change is likely to have a cost consequence for clinics. Stakeholder involvement and communications in place to ensure that clinics can feed in views before decisions are taken, and that there is awareness and buy-in in advance of any changes. Major changes are consulted on widely.	In place – Juliet Tizzard
Subjectivity of judgments means we often cannot know 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
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 being improved and updated, committee decision trees in place.	In progress and in place – Paula Robinson
HFEA process failings could create or contribute to legal	Licensing SOPs being improved and updated, committee decision trees in place.	In progress and in place –

challenges, or weaken cases that are otherwise sound, or generate additional regulatory sanctions activity (eg, legal parenthood consent).		Paula Robinson
	Up to date compliance and enforcement policy and related procedures.	In place – Nick Jones / Sharon Fensome-Rimmer
	Seeking robust assurance from the sector regarding parenthood consent issues, and detailed plan to address identified cases and anomalies.	In progress and ongoing – Nick Jones
Risk interdependencies (ALBs / DH)	**Control arrangements**	**Owner**
DH: 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 an interdependent risk because DH would be involved in resolving it.	In place – Peter Thompson
DH: Legislative interdependency.	Our regular communications channels with the Department would ensure we were aware of any planned change at the earliest stage. Joint working arrangements would then be put in place as needed, depending on the scale of the change. If necessary, this would include agreeing any associated implementation budget. The Department are aware of the complexity of our Act and the fact that aspects of it are open to interpretation, sometimes leading to challenge. Sign-off for key documents such as the Code of Practice in place.	In place – Peter Thompson

RE1: There is a risk that planned enhancements to our regulatory effectiveness are not realised, in the event that we are unable to make use of our improved data and intelligence to ensure high quality care.

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	4	16	**2**	**3**	**6 – Medium**
Tolerance threshold:					**6 - Medium**

Risk area	**Risk owner**	**Links to which strategic objectives?**	**Trend**
Regulatory effective-ness RE 1: Inability to translate data into quality	Nick Jones, Director of Compliance and Information	Improving standards through intelligence: use our data and feedback from patients to provide a sharper focus in our regulatory work and improve the information we produce	⇔⇔⇔⇔

Commentary
At tolerance. Resource strains, reflected elsewhere in this risk register, have at times affected our ability to progress the data submission project and migration activities.

Causes / sources	**Mitigations**	**Timescale / owner**
IfQ has taken longer than planned, and there will be some ongoing development work needed.	The data submission project is well planned and under way after initial delays. Data cleansing is being done to improve the quality of the data in the Register. The new Register has been designed to be easier to extract data from for analytical purposes.	Completion of data submission project March 2018 – Nick Jones
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/Dan Howard
We could later discover a barrier to meeting a new reporting need, or find that an unanticipated level of accuracy is required, involving 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. Though there has been a reduction in desktop support, there are mitigations in place to ensure day to day support, however, we are running a risk due to lack of resilience.	In place – Dan Howard
The new Intelligence team is critical to the new model, and needs to draft an information strategy before it will be possible to use the data for regulatory and other purposes.	Head of Intelligence started in September. The development of the team, and the information strategy, will follow. An Information Strategy will be produced by the new Intelligence team, to ensure that data analysis and associated internal mechanisms are in place.	In place – Juliet Tizzard In development (review by CMG in January 2018) – Caylin Joski-Jethi
Benefits of IfQ not maximised and internalised into ways of working.	During IfQ delivery, product owners were in place, and a communications plan. The changes were developed involving the right staff expertise (as well as contractors) and part of the purpose of this was to ensure that the changes are culturally embraced and embedded into new ways of working. The data submission project has been delayed but is now making good progress. Inevitably, this will impact the timeframe of benefit realisation delivery on a range of fronts.	In place (from June 2015) – Nick Jones
Insufficient capability and capacity in the Compliance team to enable them to act promptly in response to the additional data that will be available.	Largely experienced inspection team. Business support is now at full complement. Recruitment process underway for final additions to inspection team. Although not all systems are in place in relation to providing data to inspectors eg, patient feedback, workarounds are in place which are working.	In place – Nick Jones
Organisational change could take too much time to embed, the necessary culture shift may not be achieved, or new structure not accepted, with an accompanying risk to our ability to make full use of our data and intelligence as intended by the new organisational model.	Organisational re-shaping in progress, to set the right staffing structure and capabilities in place to ensure we can realise IfQ's benefits. This includes the establishment of an Intelligence team.	New organisational model in place – Peter Thompson
Regulatory monitoring may be disrupted if Electronic Patient Record System (EPRS) providers are not able to submit data to the new register structure until their software has been updated.	Earlier agreements to extend part of 'IfQ' delivery help to address this risk by extending the release date for the EDI replacement (Data submission project). 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
Data accuracy in Register submissions.	Data migration efforts are being privileged over data quality currently (Aug 2017) this is an accepted risk. The Register team has introduced a triage system to deal with clinic queries systematically. Completion of verification processes, steps in the OTR process, regular audit alongside inspections.	In place – Nick Jones
	Audit programme to check information provision and accuracy.	In place – Nick Jones
	There are 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 has improved overall data accuracy, and the exercise included tailored support for individual clinics that were struggling.	In place – Nick Jones
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. We have systems for checking consistency of answers and the flexibility to push PQ deadlines if necessary. FOI requests are refused when there are grounds for this. PQ SOP revised and log created, to be maintained by Committee and Information Officer/Scientific Policy Manager.	In place – Juliet Tizzard / Caylin Joski-Jethi
Insufficient understanding of our data and/or of the topic or question, leading to misinterpretation or error.	As above – expert staff with the appropriate knowledge and understanding in place.	In place – Juliet Tizzard / Caylin Joski-Jethi
Risk that we do not get enough patient feedback to be useful / usable as soft intelligence for use in regulatory and other processes, or to give feedback of value to clinics.	Communications strategy in place, including more patient feedback. Part of the information strategy will focus on making best use of the information gleaned from patients, and converting our mix of soft and hard data into real outcomes and improvements.	In place and to be developed – Juliet Tizzard

Risk interdependencies (ALBs / DH)	Control arrangements	Owner
None	-	-

ME1: There is a risk that patients and our other stakeholders do not receive the right information and guidance, so we miss opportunities to bring about positive change.

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
3	4	12 High	**2**	**3**	**6 - Medium**
Tolerance threshold:					**6 - Medium**

Risk area	Risk owner	Links to which strategic objectives?	Trend
Effective communications ME1: Messaging, engagement and information provision	Juliet Tizzard Director of Strategy and Corporate Affairs	Safe, ethical effective treatment: Publish clear information so that patients understand treatments and treatment add ons and feel prepared Safe, ethical effective treatment: Engender high quality research and responsible innovation in clinics. Consistent outcomes and support: Increase consistency in treatment standards, outcomes, value for money and support for donors and patients.	⇔⇔⇔⇔

Commentary
At tolerance.

Causes / sources	Mitigations	Timescale / owner
Our ability to provide patient information via the website or CaFC could be compromised by a website failure.	We have good cyber-security measures to prevent website attacks, and the new content management system is more reliable than the old one.	In place – Juliet Tizzard
Some of our strategy relies on persuading clinics to do things better. This is harder to put across effectively, or to achieve firm outcomes from.	Communications strategy in place, including social media and other channels as well as making full use of our new website. Stakeholder meetings with the sector in place to help us to underline key campaign messages.	In place – Juliet Tizzard
Our information does not meet the needs or expectations of our audience.	Ongoing user testing and feedback about the information on the website allows us to properly understand user needs. We have internal processes in place which meet the Information Standard.	In place – Juliet Tizzard
We are not able to reach the right people with the right message at the right time.	Partnering with NHS Choices to get information to patients early in their fertility journey. Planning for campaigns and projects includes consideration of communications channels.	In place and developing – Jo Triggs

	Extended use of social media to get to the right audiences.	
Some information will be derived from data, so depends on risk above being controlled.	See controls listed in RE1, above.	
Risk interdependencies (ALBs / DH)	**Control arrangements**	**Owner**
NHS Choices site and our site contain links to one another.	We maintain a relationship with the NHS Choices team.	

Reviews and revisions

Following the AGC meeting on 3 October, we have commenced a review of the risk policy and this will be reconsidered at CMG risk meeting on 22 November. We have also ensured that there is more discussion about how above tolerance risks are being managed in the summary of each risk.

In relation to AGC's comments regarding cyber security, the CIO is ensuring that all staff have completed their cyber security training by end December 2017. The executive will raise any cyber security issues to the Authority member responsible and ensure that she is updated on developments in this area.

Authority feedback – November 2017 meeting (15/11/2017)

Authority noted the report. The following point was raised:

- Authority agreed with the executive's reassessment of the organisational change risk. The residual risk has come down slightly following successful recruitments and the near completion of all planned redundancies. This meant that the risk is at tolerance. It will be removed as a separate risk once all of the organisational changes have been completed, by the end of the business year.

CMG review – November 2017 meeting (22/11/2017)

CMG reviewed the strategic risk register and made the following points in discussion:

- Members discussed the feedback from AGC about being clear about mitigations and handling of above tolerance risks and noted that we are going further to reflect action plans in the register. CMG noted the addition of a statement of risk tolerance and appetite to make the approach clearer.
- CMG discussed the C1 capability risk at length and focussed on the additional mitigations that were planned to bring this risk back to within tolerance. CMG heard that the people strategy should help with this. This would be discussed by CMG at the leadership awayday on 29 November. Alongside this, CMG heard that the Head of HR is reviewing organisational knowledge transfer methods and is preparing a corporate handover template and process. This would bolster current handover processes. The new intranet will help with signposting new staff to information, although this will not be in place as a mitigation for a number of months.
- CMG discussed the Skype issues which are ongoing and received an update from the CIO about progress on the mitigations. The CIO has been providing regular updates to the senior management team on these issues and further external resource has been identified to do additional analysis.
- When discussing the organisational change risk, CMG considered the status of organisational change recruitment and the fact that some recruitments had been harder than expected. Following discussion, it became clear that only a couple of roles were remaining, and in each case a new approach was being considered to recruiting, which should produce results. This reassured CMG that the residual score of this risk had not been reduced prematurely.
- On cyber security, members heard that staff had been reminded to complete training by end Dec 2017. A process for ongoing corporate-level oversight is being investigated but this needs to be finalised. Managers should already have oversight over the completion of mandatory training by their teams.
- Members questioned whether the likelihood of the legal risk was less than currently indicated, given that no new matters had arisen. Members agreed that it was too early to say this, but by the next CMG risk meeting in February we may wish to reassess this.

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 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

We use the five-point rating system when assigning a rating to 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

Impact	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				

Risk appetite and tolerance

Risk appetite and tolerance are two different but related terms. We define risk appetite as the willingness of the HFEA to take risk. As a regulator, our risk appetite will be naturally conservative and for most of our history this has been low. Risk appetite is a general statement of the organisation's overall attitude to risk and is unlike to change, unless the organisation's role or environment changes dramatically.

Risk tolerance on the other hand is the willingness of the HFEA to accept and deal with risk in relation to specific goals or outcomes. Risk tolerance will vary according to the perceived importance of particular risks and the timing (it may be more open to risk at different points in time). The HFEA may be prepared to tolerate comparatively large risks in some areas and little in others. Tolerance thresholds are set for each risk and they are considered with all other aspects of the risk each time the risk register is reviewed

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 introduces some element of control, even if no other mitigating action were ever taken, and even with no particular risks in mind. Therefore, for our estimation of inherent risk to be meaningful, we define inherent risk as:

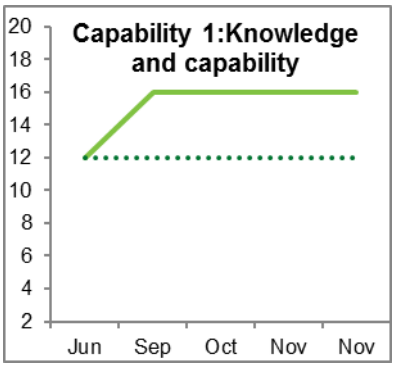
'the exposure arising from a specific risk before any additional action has been taken to manage it, over and above pre-existing ongoing organisational systems and processes.'

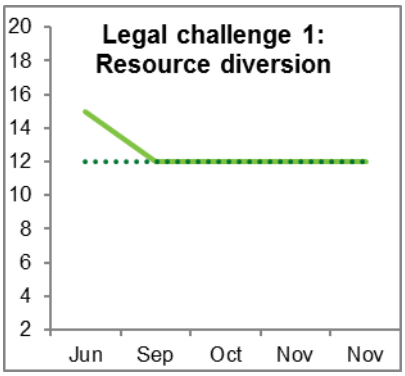
System-wide risk interdependencies

As of April 2017, we 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 has been added to the risk register, 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.

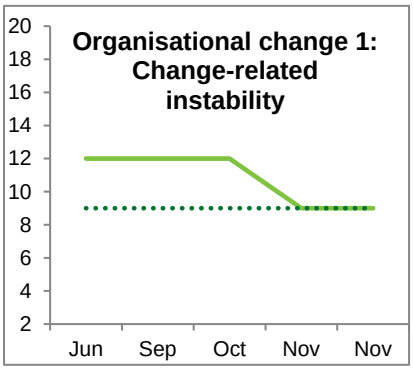
Tolerance vs Residual Risk:

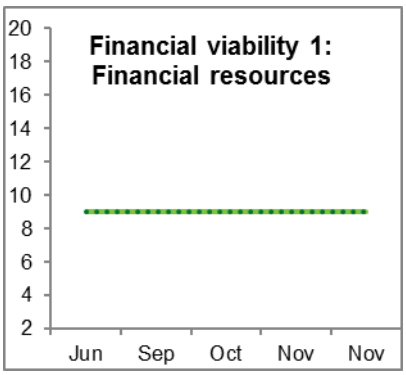
High and above tolerance risks

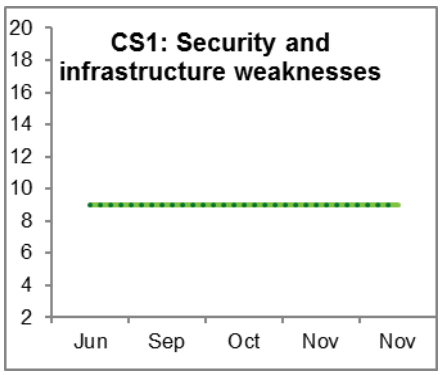


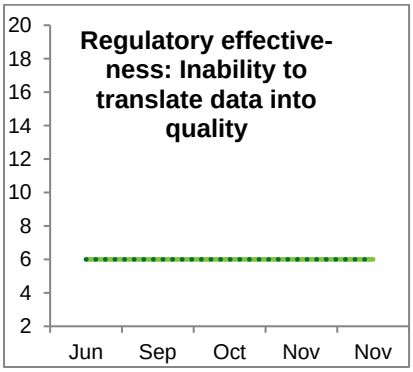


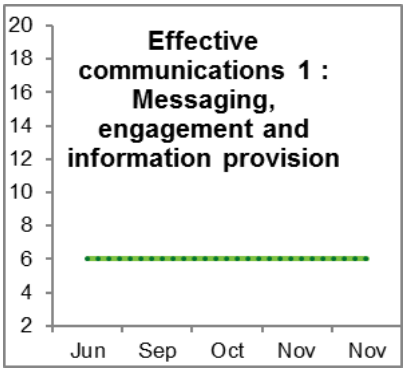
Lower level / in tolerance risks











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	12		
Paper number	AGC (05/112/2017) 582		
Meeting date	5 December 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:	6 Mar 2018	12 Jun 2018	9 Oct 2018	4 Dec 2018
Following Authority Date:	9 May 2018	27 Jun 2018	14 Nov 2018	Jan 2019
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	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	Update	Results, annual opinion approve draft plan	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:	6 Mar 2018	12 Jun 2018	9 Oct 2018	4 Dec 2018
HR, People Planning & Processes		Yes		
Strategy & Corporate Affairs management			Yes	
Regulatory & Register management				Yes
Resilience & Business Continuity Management	Yes	Yes	Yes	Yes
Finance and Resources management	Yes			
Reserves policy			Yes	
Review of AGC activities & effectiveness, terms of reference	Yes			Yes
Legal Risks			Yes	
AGC Forward Plan	Yes	Yes	Yes	Yes
Session for Members and auditors	Yes	Yes	Yes	Yes
Other one-off items				