Audit and Governance Committee meeting - agenda

5 March 2019

Chartered Institute of Arbitrators, 12 Bloomsbury Square, London, WC1A 2LP

Agenda item			Time
1.	Welcome, apologies and declaration of interests		10:00am
2.	Minutes of 4 December 2018 **[AGC (05/03/2019) 651]**	For Decision	10.05am
3.	Matters Arising **[AGC (05/03/2019) 652 MA]**	For Information	10.10am
4.	Regulatory and Register Management **[AGC (05/03/2019) 653 DH/AL]**	To Follow	10.15am
5.	Finance and Resources Update **[AGC (05/03/2019) 654 RS]**	Verbal update	10.30am
6.	Resilience, Business Continuity Management and Cyber Security **[AGC (05/03/2019) 655 DH]**	For information	10.45am
7.	Internal Audit		10.55am
	a) Audit Recommendations Follow-Up and Progress Report **[AGC (05/03/2019) 656 DH]**	For Information	
	b) Draft 2019/20 Audit Plan **[AGC (05/03/2019) 657 DH]**	For Information	
8.	Implementation of Audit Recommendations **[AGC (05/03/2019) 658 MA]**	For information	11.05am
9.	External Audit – Interim Feedback **[AGC 05/3/2019) 659 NAO]**	Verbal Update	11.10am
10.	Draft Governance Statement **[AGC (05/03/2019) 660 RS]**	For Discussion	11.20am
11.	General Data Protection Regulation Update **[AGC 05/03/2019) 661 RS]**	Verbal update	11.30am
12.	Digital Programme Update **[AGC (05/03/2019) 662 DH]**	To follow	11.35am

13.	EU Exit **[AGC 05/03/2019) 663 PT]**	Presentation	12.00pm
14.	Estates **[AGC (05/03/2019) 664 RS]**	Verbal update	12.10pm
15.	Strategic Risk Register **[AGC (05/03/2019) 665 HC]**	For Discussion	12.20pm
16.	AGC Forward Plan **[AGC (05/03/2019) 666 MA]**	For Decision	12.30pm
17.	Whistle Blowing and Fraud		12:35pm
	a) Counter Fraud and Ant—Theft Policy Review **[AGC (05/03/2019) 667 RS]**	For Decision	
	b) Whistle Blowing Policy Review **AGC (05/03/2019) 668 RS]**	For Decision	
18.	Contracts and Procurement **[AGC (05/03/2019) 669 MA]**	Verbal update	12.45pm
19.	Any other business		12.50pm
20.	Close (Refreshments & Lunch provided)		12.55pm
21.	Session for members and auditors only		12.55pm
22.	Next Meeting 10am Tuesday, 18 June 2019, London		

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 (05/03/2019) 651
Meeting date	5 March 2019
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 4 December 2018

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

Members present	Anita Bharucha (Chair) Margaret Gilmore Mark McLaughlin Geoffrey Podger
Apologies	
External advisers	Jeremy Nolan – Head of Internal Audit Rob Evans – Auditor External Audit - National Audit Office (NAO): George Smiles
Observers	Kim Hayes, Department of Health and Social Care Samantha Hayhurst, Department of Health and Social Care Ruth Wilde, HFEA Authority Member
Staff in attendance	Peter Thompson, Chief Executive Morounke Akingbola, Head of Finance 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 Clare Ettinghausen, Director of Strategy and Corporate Affairs Dan Howard, Chief Information Officer Bernice Ash, Committee Secretary

1. Welcome, apologies and declarations of interests

1.1 The Chair welcomed attendees, noting this would be Kim Hayes last meeting as she would be departing the Department of Health and Social Care (DHSC) at the end of 2018. The Committee thanked Kim Hayes for all her help and input, wishing her all the best for the future.

1.2 The Committee was informed that Nick Jones, Director of Compliance and information would be leaving the Authority, in February 2019, to take up post as Chief Executive of another professional regulatory body. The Director of Compliance and Information had been working at the Authority for eight years. The Chief Executive stated this post would be advertised shortly and he was confident of finding a good replacement. However, there was likely to be some time gap to manage, before a successful candidate would be able to commence in post, noting that PRISM should have launched by this time, but would continue to require a degree of oversight. The Chair thanked the Director of Compliance and Information for all his work during his time at the Authority. The Committee extended their thanks, wishing him well for the future.

1.3 The Committee noted apologies from Jill Hearne (National Audit Office).

1.4 There were no declarations of interest.

2. Minutes of the meeting held on 9 October 2018

2.1 The minutes of the meeting held on 9 October 2018 were agreed as a true record of the meeting 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 on-going, and others were dependent on availability or were planned for the future.

3.2 12.4,12.5 and 13.6) The Committee noted that the Strategic and Corporate Affairs presentation, the addition of Brexit and estates to the strategic risk register, alongside the addition of Brexit to the Forward Planner, would all be addressed during the course of the meeting. These items could be removed from the matters arising.

3.3 3.8) It was noted that the next training session for members would occur after the 5 March 2019 meeting.

3.4 The Committee requested an update with regard to a matter raised at the 9 October 2018 meeting, concerning the health and safety of employees driving for prolonged periods and high mileage. The Director of Compliance and Information reported this has been discussed with the inspectors and it had been identified that only a very small pool of individuals drive for inspections, as most do already travel by train. The inspectors have been asked to inform the Director of Compliance and Information if they are under any personal or family pressures which impact on their necessary mode of travel.

4. Strategy and Corporate Affairs

4.1 The Director of Strategy and Corporate Affairs spoke to the presentation, reminding the Committee of the Authority's current strategy, which concludes in 2020. The strategy for 2020-2023 will be developed in 2019.

4.2 The Committee was provided with an overview of achievements against the current strategy, noting the objectives, what has been achieved in the first eighteen months and what work is left to do. The Director of Strategy and Corporate Affairs particularly highlighted areas regarding the provision of more information to patients and additional clinic data being published in the state of the sector report. The new Code of Practice would be laid before Parliament in the coming week, taking effect in January 2019. Direct patient contact also continued to occur through attendance at events such as the Fertility Show and via our various communication channels.

4.3 Establishment of the Research and Intelligence team had enabled the state of the sector report to provide more information about clinic performance and an updated fertility trends report would be published in March 2019. Work had also been completed on a pilot national patient survey, which would be published, and findings acted upon, in due course. An updated Communications Strategy would be presented to the Authority in January 2019.

4.4 The Committee noted that the Strategy and Corporate Affairs Directorate is comprised of four teams; Planning and Governance, Research and Intelligence, Regulatory Policy and Engagement and Communications. In recent months, the Research and Intelligence team had been short of staff and also are responsible for responding to Freedom of Information requests and Parliamentary Questions. The teams also deal with approximately 2000 public enquiries annually.

4.5 Risks and trends identified for 2018 were very similar to those of 2016 and 2017. However, it was felt that the legal risk, regarding the Choose a Fertility Clinic (CaFC) function available on the HFEA website, had reduced significantly. CaFC is used regularly by patients; it had been identified that clinics require more guidance to gain an improved understanding of exactly what the available data demonstrates.

4.6 Staff turnover and capacity of key staff remains a significant risk across the Strategy and Corporate Affairs Directorate. The difficulties in recruitment, when attempting to fill vacant posts was acknowledged as more of a concern than turnover in the Directorate, resulting in current staff needing to cover more work for longer gaps. There was also a question as to whether the Authority's current communications impact is high enough, particularly as the subject area is continuously covered in the media. The implementation of the new Code of Practice would also impact on changes in clinical practice, which could be deemed a risk.

4.7 The directorate challenges were identified as being staffing, communicating what we do, using our resources and balancing quality with risk. The Committee was informed that a number of new members of staff would be joining the HFEA in January 2019. These new staff would bring new skills and approaches to the Authority. With regards to communication, it was noted that the Authority needs to consider how it can effectively participate in relevant sector conversations, particularly in light of social media platforms. The current use of old IT systems is a resource issue, particularly impacting on the licensing function of the directorate. Staff pressure, due to volume of work in some areas, was also identified.

4.8 The Committee questioned whether cash restraints prevented the Authority from conducting any particular patient campaigns. The Director of Strategy and Corporate Affairs reiterated that a Communications Strategy will be presented to the Authority in 2019 and the need to become more strategic, challenging existing assumptions about how media sources can be used, stating this is not always about cash input.

4.9 The Committee also questioned whether the resources allocated to responding to patient enquiries were always well spent. The Director of Strategy and Corporate Affairs responded saying that this was something that needed to be looked at in the light of other pressures and priorities.

4.10 Horizon Scanning was identified as a growing area, with ongoing research developments abroad, and the Committee queried whether there were enough resources available to deal with this area of work. It was acknowledged that the Scientific and Clinical Advances Advisory Committee (SCAAC) is very evidence based, looking at developments that might occur over the next three to five years. The Chief Executive reported that SCAAC is interested in cutting edge research and in identifying laboratory research which might transfer to actual use in treatment. However, it is also clear that scientific innovation can impact on success rates. In this it is important to manage the expectations of patients, a majority of which are paying for their own treatments. The absence of regulation is some countries was noted. The Chair of the Statutory Approvals Committee (SAC) spoke of the attendance of Specialist Advisors at SAC meetings, on a monthly basis, to cover expert areas, making particular references to the latest area of treatment, mitochondrial donation.

4.11 The Chair reiterated the risks identified by the Director of Strategy and Corporate Affairs, emphasising the need to question on an ongoing basis what the teams were focusing on and utilising resources effectively.

5. Internal Audit

a) Audit Recommendations Follow-Up

5.1 The Head of Internal Audit confirmed there was nothing to report to the Committee at this time.

b) Progress Report

5.2 The Head of Internal Audit stated that initial General Data Protection Regulation (GDPR) audit meeting would occur in December 2018. This work is being delivered jointly with the Human Tissue Authority (HTA) but would be reported to the Authority under separate cover.

5.3 The Committee welcomed, Rob Evans, an IT audit specialist, to the meeting, who spoke to the cyber security report. The Authority received a moderate rating for this audit. The report acknowledged there would be a move to Microsoft Azure in Summer 2019, providing an improving level of cyber security as this product incorporates good defences, noting that this would need to be monitored. The necessity to ensure other controls are in place to tackle cyber security was recognised and it was confirmed the appropriate steps are in place.

5.4 Reference was made to the management action plan, with reference to the recommendation suggesting the appointment of a non-executive member, to the Committee, who has a background in technology. Noting that there would be no further recruitment to the Committee at this time, it was agreed this is an element for consideration when next seeking to appoint external members. The Committee noted that independent advice could be sought as necessary alongside the continuous evolution of technology, which impacts on an individual's 'expertise'. The Director of Compliance and Information stated that independent advice is gained when necessary and had been a valuable resource for the PRISM project. Cyber Security is a regular item on the Committee's agenda and reported to the Authority.

5.5 The Committee acknowledged that the recommendation concerning the addition of cyber security to the Strategic Risk Register had already been actioned. There was also a recommendation that consideration should be given to introducing denial of service prevention such as Akamai, as a tactical mitigation ahead of the completion of the migration to Microsoft Azure. The Chief Information Officer assured the Committee that this had been carefully considered and based on the risk, it had been decided to not pursue this at the current time and this will be revisited during summer 2019. The Chief Executive spoke of the risk pertaining to the Authority being without data for a period of time, in the event of IT systems becoming unavailable, stating these can be managed.

5.6 The Chair thanked Internal Audit for the timely report, which had been beneficial.

6. Implementation of recommendations

6.1 The Head of Finance reported there are 14 outstanding audit recommendations, with seven remaining open. The HR policy and procedures regarding appointment of temporary promotions should be completed in January 2019. A policy statement concerning the recovery of overpayments that directly links to the overarching Debt Recovery Policy should also be drafted and shared early in 2019. The Committee questioned whether the policy on temporary promotions should explicitly state these appointments will be for specific tasks.

6.2 The Chair expressed some concern that the completion date for the audit recommendation, concerning data loss, has been pushed back several times. The Chief Information Officer stated this would be completed at the earliest possible time after the Christmas period.

6.3 The Head of Internal Audit informed the Committee that the Authority is in a good position in relation to the implementation of the recommendations and there are no concerns.

7. External Audit – audit planning report

7.1 The NAO reported that the two risks, which have the most significant impact on the audit, have been identified as the management override of controls and revenue recognition. Assets under construction (PRISM) and exiting the European Union has been identified as the two areas of audit focus. With regards to materiality, the error reporting threshold would remain at £2,500.

7.2 The NAO asked the Committee to confirm that there was nothing to bring to their attention with concerning fraud; the Chair formally confirmed there were no items of fraud to report.

7.3 The NAO confirmed that Jill Hearne had taken over Sarah Edward's position, dealing with audit for the Authority. The timetable for reporting has been established. It was noted that the Committee meeting date, for the June 2019 meeting, had been moved forward to 18 June 2019 to ensure all documentation regarding the audit of the annual report and accounts was ready for presentation.

8. General Data Protection Regulation update

8.1 The Director of Finance and Resources reported there are a small number of outstanding issues, none of which are high risk. Some documentation containing personal data might still be in existence and this would be dealt with in 2019. The incompletion of the Retention Policy poses a small risk.

8.2 The Director of Finance and Resources stated that the migration of data would be occur on April/May 2019, after which time, information no longer required would not be held. A further update on GDPR progress would be presented to the Committee in due course. It was also noted that there would be an internal audit of the Authority's GDPR compliance undertaken in the last quarter of the 2018/19 business year.

9. Digital Programme update

9.1 The Chief Information Officer spoke to the paper and presentation, providing a digital programme update, particularly referencing the issues encountered with stage 2 of the PRISM data migration.

9.2 The Committee acknowledged there had been a good level of engagement with the sector and EPRS suppliers and it was highlighted that the stage 1 transfer of data had resulted in excess of 99% of data being migrated into the new register, excluding gamete movements. With regards to stage 2 of the data migration, initial testing of data shows between 94%-100% correct matches. However, the algorithm required for CaFC and Gamete Movement (EggBatchID) is taking significantly longer than expected to develop. This had delayed the launch of PRISM to January 2019.

9.3 The website's CaFC function provides a performance view of clinics, including success rates and is typically updated every 6 months. The last update was conducted 2 years ago, creating a backlog of data for clinics to check prior to the go live date; the register team will closely support clinics with this exercise.

9.4 The Chief Information Officer reported there will be additional capital and revenue costs to support the final migration and launch in January 2019 and a meeting was planned to look at the budget for this work. The Director of Finance and Resources confirmed that any additional costs would be absorbed within the capital allowance figure approved by DHSC earlier this year. Any further issues regarding PRISM will be reported to the Committee as necessary.

9.5 Noting the slippage with regards to the launch of PRISM, the Committee asked if the Authority is being too ambitious in stating a January 2019 introduction date. The Chief Information Officer stated that the current register could be used for as long as necessary, but the main passage of PRISM work had been completed and a January launch date is feasible. The Chief Executive expressed that there will always be some element of further data checking required. If some fields of information contain minor inaccuracies, there is no significant issue with launching the new register.

9.6 The Chief Information Officer stated that it was hoped the deferred teleconference, to attain approval to proceed with the launch of PRISM, could be rescheduled for the week beginning 7 January 2019, checking on members availability. One Committee member confirmed he would not be available during this time period but would be content to comment by email.

9.7 It was acknowledged that, with regards to Parliamentary Questions (PQs), there is a good match between the live Register and the migrated data, but some differences do exist. This creates a risk that responses to PQ's, using migrated data, will be inconsistent pending reconciliation, and this needs to be addressed. The Director of Strategy and Corporate Affairs stated that PQ answers are submitted on the basis that data is correct as of a given date. The Department of Health and Social Care (DHSC) stated that it was appreciated that information is a constantly moving object and accepted this as a principle for answering PQs.

9.8 The Chair thanked the Chief Information Officer for the update on PRISM and the assurances provided.

Action

9.9 The Committee to attend a teleconference, during the week beginning 7 January 2019, prior to the launch of PRISM, to attain approval to proceed. Any Committee members unable to attend would submit their comments by email.

10. Resilience, business continuity management and cyber security

10.1 The Chief Information Officer provided an update with regard to resilience, business continuity and cyber security, speaking to the paper and providing a presentation.

10.2 The Committee noted that the internal IT team had been concentrating their work on Authority specific support issues. Alscient had been used since April 2018 for maintenance of infrastructure and migration work. A 6 month extension has been agreed, pending a market review. A procurement exercise will occur in early 2019 to engage the market to secure a longer-term arrangement. This is likely to involve procuring via the Crown Commercial Services Framework, which can access around 45 suppliers. The timeline for this work was acknowledged.

10.3 Work to upgrade the phone and video-conferencing facilities is ongoing, with an expected completion date of January 2019. These upgrades cannot give absolute assurance that all current issues will be completely eradicated, but there will be fewer reasons for failure. The Committee noted that these new video-conferencing facilities can be accessed from anywhere, not just in specific rooms at Spring Gardens. The Committee agreed that it would be useful for all meeting and Authority members to be issued with some operational guidance, informing them of the minimum IT standards/equipment they require to join video-conferences.

Action

10.4 All Committee/Authority members to be issued with video-conferencing operational guidance and necessary information regarding the minimum IT standards/equipment required.

11. HR Issues

a) Organisational Capability and HR Report

11.1 The Chief Executive spoke to the paper, principally addressing the issue regarding staff turnover. He reiterated that the recruitment of new staff can bring in new ideas and enthusiasm; however, staff departures do create a loss of expertise and corporate memory, and place extra work on existing staff whilst the recruitment exercise is conducted.

11.2 Twenty individuals had left the Authority over the last 12 months, 13 of which had been resignations from staff who had worked for the organisation for over three years, accounting for 76% of the total. The Committee was informed that exit interviews are conducted, on a voluntary basis, and 18 of these have been conducted since June 2017. The top three reasons given for leaving were lack of opportunities for progression, pay and relationships with a line manager. It was noted that 52% of staff are in Band 3, reflecting the specialist work of the Authority. The constraints of public sector pay does have an impact for some staff but was not consistently reported.

11.3 The Committee noted that a range of issues had been identified at the last staff awayday, held in December 2017, following the annual staff survey, and actions had been taken to address areas of learning and development, rewards, internal communications (partly addressed by the launch of the intranet) and culture.

11.4 The Chief Executive recognised that the key drivers for turnover are unlikely to change in the short to medium term, particularly in relation to pay. The speed of the recruitment process has improved, but it still proved difficult, in some cases, to attract suitable candidates for vacancies. Advertising roles through the NHS and Civil Service jobs is not always the best platform for recruitment. Job Bands at the Authority are wide and allow few opportunities for advancement, but more senior positions might be able to be identified within these. It was acknowledged that the wider benefits of working for the public sector need better articulation i.e. the civil service pension and flexible working. There was also a recognition that the work of the Authority is interesting, valuable experience can be gained at the organisation, and there is the potential of career development across the public sector.

11.5 The Chair noted that the issues discussed will continue to be a feature, creating challenges for the Authority. It would be useful for the Committee to receive information about any specific initiatives being used to address organisational capability.

11.6 The Committee echoed the issues caused by such a high percentage of staff being within Band 3 and the lack of available progression. There was also a question pertaining to how many staff stay in post and have no specific ambition to advance their careers. New employees should be able to join the organisation with the prospect of advancing to a higher role. There was a need to create greater opportunities for advancement within the Band structure.

11.7 The Chief Executive stated that legacy planning does occur in an informal manner, through Personal Development Plan (PDP) conversations. The Director of Strategy and Corporate Affairs noted the need to support staff careers. Reference was also made to flexible working, which could be used in variable ways, including enabling staff to partake in further studies.

11.8 The Committee expressed concern, regarding some of the social aspects of working for the Authority, noting there is no communal area for staff to meet, within the current premises. The Chief Executive confirmed that all staff meetings occur on a monthly basis. The next awayday would take place on 10 December 2018, where the results of the most recent staff survey would be discussed, and actions identified. Following this event, the results of the staff survey would be shared with the Committee.

Action

11.9 The results of the staff survey to be circulated to the Committee, following the 10 December 2018 staff awayday.

12. Brexit

12.1 The Chief Executive recognised that the Parliamentary vote on Brexit would occur on 11 December 2018 [NB. now delayed]. If the deal is supported, the transitional stage will ensure little or no change for some time. However, if the deal is rejected by Parliament, it is unclear what the next moves would be.

12.2 The DHSC reported that it was now a requirement for all organisations to have a nominated staff member in charge of Brexit and it was confirmed that the Director of Compliance and Information currently filled this position for the Authority.

12.3 The Chief Executive informed the Committee that clinics were all aware of the technical notes and communications with them on Brexit continued. The possible impact of Brexit on the supply of drugs, equipment and storage was noted and the sector needs to have contingency plans in place.

12.4 The DHSC had been told to continue with no Brexit deal preparations until all documentation has been passed by the EU Parliament. Nothing would be definite until March 2019. No Brexit deal regulations were laid before Parliament on 19 November 2018 and the Authority will be informed when these are passed. The new regulations will take effect after a transitional period in the event of a no deal scenario.

13. Estates

13.1 The Director of Finance and Resources reported that the issue of estates was progressing well and that the initial recommendations of the DHSC London Office Strategy Steering Group would go forward for consideration by the Department’s Director General Finance – David Williams. The proposals place the HFEA in the Stratford Hub, although this location for the office move could still change as the project goes through Cabinet Office and Full Business Case approval.,

13.2 The Committee noted that until any new property is cleared and signed off by the Cabinet Office, a degree of uncertainty would remain. The project was expected to be given final approval by DHSC at the end of March 2019 and it was confirmed that they would be funding the move. Once the new office venue had been confirmed, a project group would be convened to explore all aspects of the move including finances, logistics and cultural change.

14. Strategic Risk Register

14.1 The Risk and Business Planning Manager presented the strategic risk register.

14.2 The Committee noted that SMT reviewed the strategic risk register on 19 November 2018 and there was a full discussion regarding the tolerance level for the cyber risk, noting this had been above tolerance since July 2018. SMT agreed that the Authority is not 'above tolerance' for cyber security, although the environment had changed and therefore the Authority's tolerance had increased slightly to 9. The Committee felt that the risk score could be viewed as somewhat low. The Director of Compliance and Information stated there would always be a residual risk and members asked whether the Authority had undertaken all the actions it could reasonably be expected to conduct. The Chief Information Officer confirmed that, based on information held and the current controls, there was no reason to think that a higher residual risk rating was necessary for cyber security.

14.3 SMT had discussed the business continuity arrangements and plans, identifying there had been no business continuity test since September 2017. It was agreed that another test would be arranged.

14.4 The Committee noted that the estates risk had been incorporated into the Strategic Risk Register, under the Capability risk. The Risk and Business Planning Manager stressed that the nature of the risks around the office move would become clearer over time and this risk would be expanded, to ensure that all risks and risk interdependencies were captured.

14.5 The Committee recognised that a significant amount of work had been conducted on Standard Operating Procedures (SOPs), congratulating the Authority on this.

15. Reserves Policy

15.1 The Director of Finance and Resources introduced the Reserves Policy, referring to the increasing cash balance and the reasons for the continuing surplus. The Committee noted that, by default, the Authority is required to make a small surplus each financial year. The agreement with the sponsor department is that the Authority's finances will never exceed the total amount of income plus Grant-in-Aid.

15.2 Cash holdings also increase due to the non-cash expenditure each year. However, this has now been rectified by ensuring that non-cash costs are covered by the department and are ring fenced.

15.3 If a surplus continues to be made, the cash holding will also increase dependent on the size of the annual surplus; a 1% surplus equates to a £60k increase in cash.

15.4 A number of options had been identified with regards to reducing the Authority's cash balance including returning cash to the General Fund, returning an element of fees back to stakeholders and investment in infrastructure and funding wider programmes. It was identified that all of these available options have some issues attached.

15.5 The Director of Finance and Resources reported that the options to return cash to the General Fund and give an element of fees back to stakeholders had not been ruled out, but there was the potential preference for surplus cash to be used to fund key projects. The Chair agreed this is an option for further investigation.

15.6 The DHSC stated that surplus cash would only be reclaimed as a last resort. The Committee agreed that it would be ideal if the surplus cash could be utilised for a project benefiting the patient community. The DHSC would support this as a general principle and consider any project ideas presented.

15.7 The Committee approved the Reserves Policy, requesting any update on the usage of surplus cash, to be presented at a future meeting, in due course.

Action:

15.8 The Committee to receive an update on the usage of surplus cash, in due course.

16. AGC forward plan

16.1 The Head of Finance reported that, due to some items being deferred to later meetings in 2018, including the annual Regulatory and Register Management update, the Forward Planner for 2019 is quite full. The Chair stated the Forward Planner should be sufficient, but items can be moved to later dates, if necessary. The Committee agreed that it would be useful to receive a draft governance statement at the 5 March 2019 meeting.

Action: The Committee to receive a draft governance statement at the 5 March 2019 meeting.

17. Whistle blowing and fraud

17.1 The Director of Finance and Resources informed the Committee there were no cases of whistle blowing or fraud to report since the last meeting.

18. Contracts and procurement

18.1 The Head of Finance reported that, since, the last meeting, one contract had been extended and a new one had been entered into for the DMS.

19. Review of AGC activities & effectiveness, terms of reference

20.1 The Committee Members discussed this item in a private session.

20. Any other business

20.1 Members and auditors retired for their confidential session.

20.2 The next meeting will be held on Tuesday, 5 March 2019 at 10am.

21. Chair's signature

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

Signature

Name

Anita Bharucha

Date

5 March 2019

Audit and Governance Committee Paper

Paper Title:	**Matters arising from previous AGC meetings**
Paper Number:	**[AGC (05/03/2019) 652 MA]**
Meeting Date:	5 March 2019
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:

- 5 items added from December 2018 meeting, 2 ongoing
- 6 items carried over from earlier meetings, 5 ongoing

ACTION	RESPONSIBILITY	DUE DATE	PROGRESS TO DATE
Matters Arising from the Audit and Governance Committee – actions from 12 June 2018 meeting			
9.10 The Committee to receive monthly updates highlighting any variances and increased risk.	Chief Information Officer		**Ongoing**
9.11 There would be joint approval between the Committee and key staff for data migration sign off, with full assurance being provided concerning the move of the Register to the Microsoft Azure 'cloud'.	Chief Information Officer		**Ongoing**
9.12 Any further significant issues would be addressed through a meeting with the Committee Chair and key staff.	Chief Information Officer		**Ongoing**
Matters Arising from the Audit and Governance Committee – actions from 9 October 2018 meeting			
3.8 The Committee Secretary to contact members regarding availability for training after the meeting on 4 December 2018 or 5 March 2019	Committee Secretary		**Ongoing -** Training will occur after the June 2019 meeting.
8.13 The Committee to receive a further paper on the digital programme, which would be followed-up by a teleconference, prior to the launch of PRISM, to attain approval to proceed.	Chief Information Officer		**Ongoing**
11.7 The Risk and Business Planning Manager to circulate a final version of the	Risk and Business Planning Manager		**Complete –** Circulated on 16 January 2019

risk policy to the Committee, following the 14 November Authority meeting.			
Matters Arising from the Audit and Governance Committee – actions from 4 December 2018 meeting			
9.9 The Committee to attend a teleconference, during the week beginning 7 January 2019, prior to the launch of PRISM, to attain approval to proceed. Any Committee members unable to attend would submit their comments by email.	Chief Information Officer		**Ongoing –** relates to items 9.11, 9.12, 8.13. Approval not sought as work continues to resolve key issues.
10.4 All Committee/Authority members to be issued with video-conferencing operational guidance and necessary information regarding the minimum IT standards/equipment required.	Chief Information Officer		**In progress –** testing of new systems is underway. Once tests completed, guidance will be created/tested and shared with Committee.
11.9 The results of the staff survey to be circulated to the Committee, following the 10 December 2018 staff awayday.	Chief Executive		**To be provided at the meeting.**
15.8 The Committee to receive an update on the usage of surplus cash, in due course.	Director of Finance and Resources		**Verbal update –** to be given at the meeting
16.1 The Committee to receive a draft governance statement at the 5 March 2019 meeting.	Head of Finance		**Provided in meeting pack**

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 (AGC)		
Agenda item	6		
Paper number	AGC (05/03/2019) 655 DH		
Meeting date	05 March 2019		
Author	Dan Howard, Chief Information Officer		
Output:			
For information or decision?	For information		
Recommendation	The Committee is asked to note: • The update on procurement to secure a supplier for essential IT infrastructure and development support; • The update on work to upgrade our telephone system, network and video-conferencing facilities; and • The approach to refresh information risk training and business continuity plan testing		
Resource implications	Within budget		
Implementation date	Ongoing		
Communication(s)	Regular, range of mechanisms		
Organisational risk	☐ Low	☒ Medium	☐ High
Annexes:	None		

1. Introduction and background

1.1. In recent months, AGC has received regular and detailed updates on Resilience, Business Continuity Management and Cyber Security, in line with the strategic risk register.

1.2. In December 2018 AGC received an update on our IT infrastructure and IT development support arrangements. We signalled an intention to secure a longer term support arrangement in 2019. The associated procurement work is progressing well and an update on progress is below.

1.3. In December 2018, AGC also received details on our plan to make improvements to our telephone system and video-conferencing facilities. An update is available below.

1.4. Our Business Continuity arrangements are continually under review and routine testing is scheduled to take place shortly involving all staff.

1.5. Information risk training is undertaken on a regular basis and we regularly review our provision. The e-learning training has recently been updated and will be undertaken by all staff during March and April 2019.

2. IT infrastructure support

2.1. In December 2018, AGC received an overview of our strategy setting out a plan to source IT infrastructure and system support – such as for the Office 365 infrastructure, certain hardware such as generic network components and some system monitoring, to a third party.

2.2. A detailed review has taken place. The review identified a requirement for first and second line support for several key areas such as user account management, support for Microsoft Virtual Machine and Azure servers, management of specialist databases, website management, support for specialist systems such as our licensing system. Our inhouse team will continue to concentrate on supporting HFEA-specific systems and the HFEA-specific configuration of enterprise systems.

2.3. We plan to go to market using Crown Commercial Services framework RM3745, lot 8. This provides access to around 45 suppliers and we expect around 6-10 to bid.

2.4. The full suite of procurement documents will be reviewed by Corporate Management Group on 20 March 2019, we expect to go to market thereafter and we will report the outcome to AGC in due course.

3. Telephone system and video conferencing upgrades

3.1. In December 2018 AGC received an update on our work to improve our telephony system, network and associated infrastructure. This upgrade will deliver significant benefits: providing the network capacity we require, supporting improvements to video-conferencing, aligning to our 'cloud first' IT strategy and enabling a smooth transition to new premises in 2020.

3.2. Telephone numbers have been ported into the new service and the server improvements - moving the Skype for Business server from on-premise to cloud data-centre is complete. The bandwidth improvements (from 100Mb/second to 200Mb/second) are scheduled to take place on 13 March 2019.

3.3. Detailed testing for five test users is underway. Initial feedback is very positive; call quality, video quality and document sharing is functioning as expected and user feedback is good.

3.4. Once testing is complete we will incrementally transition all users into the new service, and review effectiveness and capture feedback.

4. Recommendation

The Committee is asked to note:

- The update on procurement to secure a supplier for essential IT infrastructure and development support;
- The update on work to upgrade our telephone system, network and video-conferencing facilities; and
- The approach to refresh information risk training and business continuity plan testing

Audit and Governance Committee

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

Details:

Meeting	Audit & Governance Committee
Agenda item	7
Paper number	AGC (2019-03-05)
Meeting date	5 March 2019
Author	Jeremy Nolan

Output:

For information	To provide an update to the Audit and Governance Committee on the 2018/19 Internal Audit Plan and seek approval for the draft 2019/20 Annual Audit Plan.
Progress Update	**Progress on 18/19 Audit Plan** **Cyber Security –** The final report for this review has been issued, with a moderate assurance rating given. **Business Continuity Planning** – The fieldwork for this review was delayed, due to key information not being provided. The draft report for this review is expected to be issued W/C 4th March. **GDPR Review** – The fieldwork for this review has now been completed. The draft report for this review is expected to be issued W/C 11th March. **Anti Fraud Controls** – The fieldwork for this review has now been completed. A draft report for this review is attached is expected to be issued W/C 4th March. **Recommendations Follow Up** – Internal Audit have been working closely with HFEA to resolve all outstanding recommendations from previous audit reviews. Progress has been made and we continue to have regular communications to ensure appropriate action has been taken to implement all recommendations. **2019/20 Audit Plan** – The proposed audit plan for 2019/20 is attached for your consideration and agreement.

Actions from previous meeting	None		
Organisational risk	☐ Low	☒ Medium	☐ High
Annexes	Annex A – Draft 2019/20 Audit Plan Annex B – Previous Years' Internal Audit reviews (for information)		

Government
Internal Audit
Agency

Human Fertilisation and Embryology Authority (HFEA)

2019-20 Internal Audit Plan

Draft

Date of issue:	February 2019

This document has been prepared for, and is only for HFEA management and staff. HFEA must consult with GIAA (pursuant to part IV of the Secretary of State Code of Practice issued under section 45 of the FOI Act) before disclosing information within the reports to third parties. Any unauthorised disclosure, copying, distribution or other action taken in reliance of the information contained in this document is strictly prohibited. The report is not intended for any other audience or purpose and we do not accept or assume any direct or indirect liability or duty of care to any other person to whom this report is provided or shown, save where expressly agreed by our prior consent in writing.

Overview

The main purpose of Internal Audit is to provide the Accounting Officer with an independent, objective evaluation of, and opinion on, the overall adequacy and effectiveness of the organisation’s framework of governance, risk management and control.

As Chief Internal Auditor, I am responsible for:

- developing a strategy to meet the main purpose of the internal audit activity;
- establishing risk-based internal audit plans, consistent with the organisation’s goals; and
- providing an Annual Opinion on the adequacy and effectiveness of the organisation’s systems of risk management, governance and control.

This paper sets out:

- our audit strategy;
- our approach to developing the internal audit plan;
- our internal audit plan for 2019-20.

Our Audit Strategy

We will deliver our internal audit service to you in accordance with the GIAA Charter and with the Public Sector Internal Audit Standards (PSIAS). Copies of both documents are available on request.

Our internal audit plan and activity will link to your organisation’s objectives, risks and priorities and provide assurance over the adequacy and effectiveness of governance, risk management and control. This assurance will be risk-based and reasonable, but not absolute, in its coverage.

We will deliver our services through a blend of resources that are appropriate, sufficient and effectively deployed to achieve the plan. Where appropriate, we will place reliance on the work of other assurance providers.

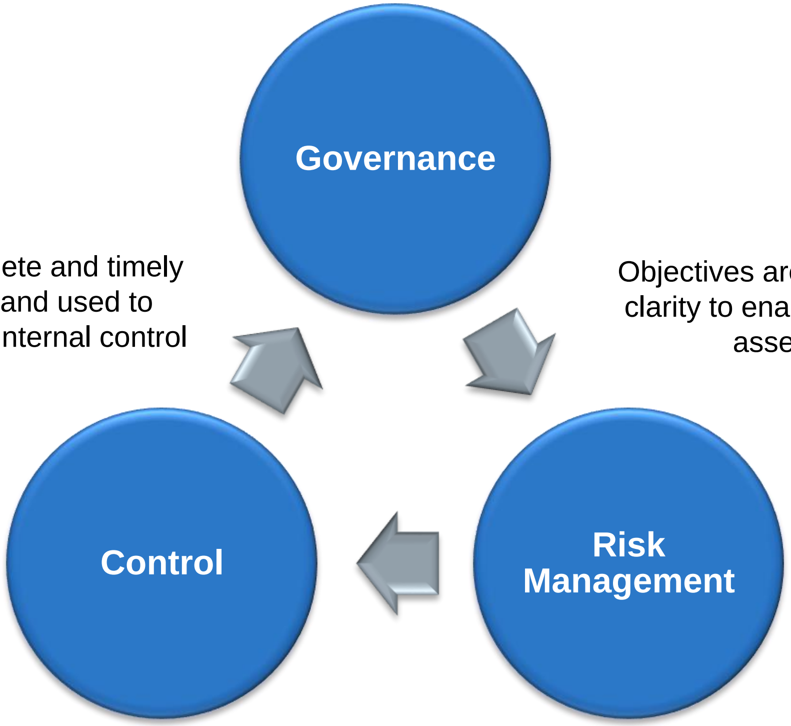
We will maintain a quality assurance and improvement programme that covers all aspects of our internal audit activity. We will report the results of our quality assurance and improvement activity in the annual assurance report.

We will deliver products including:

- engagement reports throughout the year, according to the timings in the plan;
- reports to each meeting of the Audit and Governance Committee (AGC) on significant risk and control issues and progress against the plan; and
- an annual assurance opinion and report.

The Purpose of the Internal Audit Plan

The plan is designed to evaluate the extent to which:



Oversight, structures, authorities and responsibilities, and reporting support a clear understanding of risks and controls and effective decision-making.

Governance

Objectives are specified with sufficient clarity to enable the identification and assessment of risks.

Risk Management

Risks to the achievement of objectives are identified and assessed to determine how they should be managed.

Changes that could significantly affect the system of internal control are identified and assessed.

Control

Control activities are designed adequately and operated as intended to mitigate risks to acceptable levels.

Relevant, accurate, complete and timely information is available and used to support the functioning of internal control

Our Approach to Developing the Plan

In accordance with the PSIAS, we prepared the plan on a risk basis and considered:

Your objectives and priorities

We reviewed your objectives and priorities from your business plan and, where available, other sources.

How risks impact on your business

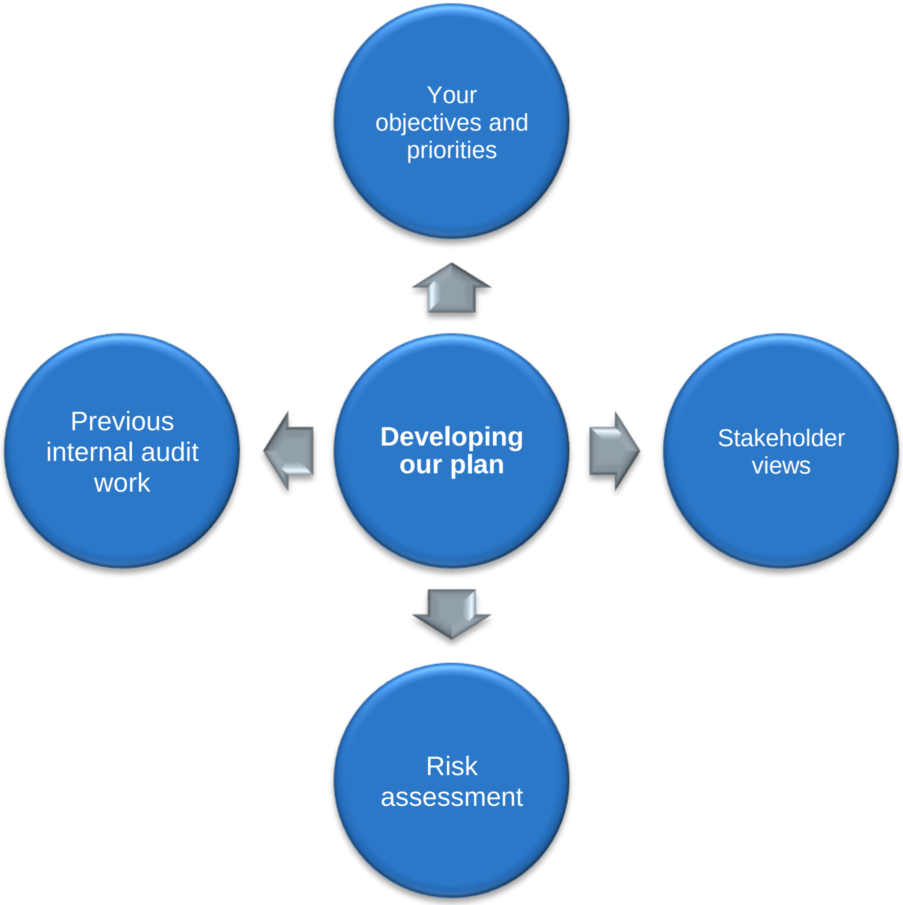
We assessed the risks to achievement of your objectives and priorities, given the controls you have in place. Where available, we reviewed your risk register.

Stakeholder views

We engaged with stakeholders, including Senior Responsible Officers, Directors and Executive Team members.

Previous Internal Audit Work

We reviewed the findings of our previous internal work. Where available, we reviewed your assurance framework. Where appropriate, we reviewed the work of other assurance providers.



Coverage by Risk Area

Our plan provides for coverage of the risk areas shown in the chart. These areas are defined at Annex 1.

Our plan also provides for coverage of the risks within your risk register, as shown in the table.

Risk register	Relevent Audit Activity to be Undertaken
FV1: There is a risk that the HFEA has insufficient financial resources to fund its regulatory activity and strategic aims.	Annual Budgeting Processes, Corporate Governance
C1: There is a risk that the HFEA experiences unforeseen knowledge and capability gaps, threatening delivery of the strategy.	External Information Requests, Risk Management of Capability Risks, Corporate Governance, Records Management
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.	External Information Requests, Corporate Governance
LC1: There is a risk that the HFEA is legally challenged given the ethically contested and legally complex issues it regulates.	Corporate Governance
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.	Corporate Governance
ME1: There is a risk that patients and our other stakeholders do not receive the right information and guidance from us.	External Information Requests, Corporate Governance, Records Management

Internal Audit Plan 2019-20

Audit title	Outline Scope	Days	Timing	Risk Area
External Information Requests	To assess how effectively HFEA manage and mitigate the risk that incorrect information is provided in PQs, OTRs or FOIs.	10	Q2	C1, ME1
Risk management of capability risks	We will examine the extent to which HFEA are implementing the capability risk mitigations shown in the strategic risk register, and review the effectiveness of the associated assurance arrangements.	10	Q1	C1
Corporate Governance	This review will look at the effectiveness of governance structures and associated accountability arrangements.	10	Q3	Spans all risk areas
Records Management	A review of records management processes and policy within HFEA, including how it deals with document retention, security and retrieval of archived material in order to fulfil its legal and operational requirements	10	Q4	C1, ME1
Annual Budgeting Process	This review will look at how risks relating to budget planning are mitigated by HFEA, including risks around income estimation, complying with spending controls and other risks outlined in the strategic risk register.	10	Q2	FV1

Internal Audit Plan 2019-20

Audit title	Outline Scope	Days	Timing	Risk Area
Management Time	This is time for the Head and Deputy Head of Internal Audit, and includes activities such as annual audit planning and preparation and attendance at ARAC meetings.	10		
Contingency		4		
Recommendations Follow Up		1		
		65		

Annex 1: Risk Areas

Risk Area Description	Elements included	
Strategy Risk - Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data, assumptions and/or intelligence, and/or fails to support the delivery of commitments and/or objectives.	Strategy alignment Research, insight and intelligence	Forecasting and analysis Assumptions
Governance Risk - Risks arising from unclear plans, authorities and accountabilities and/or ineffective or disproportionate oversight of decision making and/or performance.	Planning Authorities and accountabilities	Scrutiny and challenge
Operations Risk - Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, non-compliance with regulation or legislation, impaired customer service and/or poor value for money.	Product/service design, development and improvement Operational processes	Operational performance Customer communication
Financial Risk - Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, non-compliance with financial regulation, legislation and standards.	Financial planning and forecasting Funding Financial & budgetary management Payments	Debt management Tax Accounting and reporting
Commercial Risk - Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, failure to meet business requirements, non-compliance with regulation and legislation.	Procurement Business specification Market failure	Contractual award Demand management Contract management
People Risk - Risks arising from ineffective leadership and engagement, the unavailability of sufficient capacity and capability, industrial action, non-compliance with regulation and legislation or internal HR policies.	People strategy and planning Managing organisations Joining work Building the workforce	Managing the workforce Rewarding the workforce Leaving work Managing HR services
Technology Risk - Technology does not deliver the expected services due to inadequate or deficient system/process development and performance.	System application development Platforms System performance	Maintenance and support Service resilience and continuity
Information Risk - Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.	Integrity of information Availability of information	Exploitation of information
Security Risk - Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate or information, non-compliance with regulation and legislation.	Physical security Information security	
Programme and Project Risk – Risks that programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver to time, cost and quality.	Strategic alignment Programme and project plans Management information Programme and project delivery	Business impact Benefit realisation Programme and project governance Stakeholder engagement

HFEA: Summary of Previous Audit Work

Topic	Scope	2013/14	2014/15	2015/16	2016/17	2017/18	2018/19
Strategy/Compliance							
Francis and McCracken	Robust arrangements are in place to respond to the recommendations of the Francis and McCracken reports.	Y					
Corporate Governance	An assessment of the efficacy of key HFEA committees	Y					
Risk Management	Review and testing of the arrangements in place for managing risk at all levels across HFEA, including monitoring, filtering and escalation processes.	Y					
Internal Policies	Review of the HFEA's arrangements to monitor, review and refresh key policies, procedures and terms of reference.		Y				
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.					Moderate	
Operational							
Requests for information	Review of policies and procedures in relation to Parliamentary Questions (PQs), Freedom of Information (FOI) requests and Data Protection (DP) requests.			Y			
Incident Handling	Review of current policies and procedures relating to incident and complaints reporting and responses			Y			
Business continuity							Not complete
Financial							
Payroll and expenses	Accuracy and completeness of payments payroll and expense payments. Compliance with HMRC rules of payments for expenses and emoluments made to committee members	Y					Moderate
Standing Financial Instructions	Assurance over current standing financial instructions, including a comparison with HFEA's existing arrangement versus good/best practice.		Y				
Income generation process/ quality and efficiency of revenue data	Assessment of income generation and invoicing process from receipt of the electronic treatment forms from clinics to the raising of an invoice.				Moderate		
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.					Substantial	
Anti Fraud Controls							Not complete
Information Technology							
Information for Quality	Assurance over the IfQ programme using PwC's 'Twelve Elements Top Down Project Assurance Model'.		Y				
Register of treatments	'Critical friend' input into key project meetings in relation to the migration of data to the new register of treatments.		Y				
Data migration – Register of treatments	'Critical friend' input into the work performed by the HFEA to migrate data to the new Register of Treatments database. Testing a sample of data between the old and new Registers to verify the accuracy and completeness of data.			Y			
Information Standards	Information governance standards in relation to corporate information				Moderate		
Board effectiveness	This was a high level review to assess the Board effectiveness via a self-assessment survey and follow-up interviews.				Not rated		
Cyber security	Concerned security risks relating to a cloud environment and identifying any gaps in HFEA's security control framework.				Moderate		Moderate
Data Loss	This review will be undertaken to review the controls around the key risk that HFEA data is lost, becomes inaccessible, is inadvertently released or is inappropriately accessed.					Moderate	
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.					Advisory	Not complete

Human
Fertilisation &
Embryology
Authority

Progress with Audit Recommendations

Strategic delivery:	☒ Setting standards	☐ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item	Progress with Audit recommendations		
Paper number	AGC (05/03/2019) 658 MA		
Meeting date	5 March 2019		
Author	Morounke Akingbola, Head of Finance		
Output:			
For information or decision?	For information		
Recommendation	The Committee is asked to Note: there are 14 outstanding audit recommendations of which 4 remain open. Since the last meeting there has been two further audits not included in the Tracker (GDPR and Anti-Fraud). Committee to note completed audits will be removed on confirmation from Internal Audit adequate evidence has been provided.		
Resource implications	None		
Implementation date	During 2018-19 and 2019-20 business year		
Communication(s)	Regular, range of mechanisms		
Organisational risk	☐ Low	☒ Medium	☐ High

SUMMARY OF AUDIT RECOMMENDATIONS

Year of Rec.	Category	Audit	Section	Rec #	Recommendations	Action Manager	Proposed Completion Date	Complete this cycle?	Evidence
2018/19	Moderate	DH Internal Audit	Payroll and Expenses	1	Inadequate policies and procedures	Morounke Akingbola, Head of Finance and Facilities Yvonne Akinmodun, Head of HR	October 2018	Yes	Copy T&S Requested 20 Jan
				2	Incorrect payments to starters and leavers	Yvonne Akinmodun, Head of HR	October 2018	Yes	Requested 20 Jan
				3	Inappropriate expense claims paid	Richard Sydee, Director of Finance (Morounke Akingbola, Head of Finance)	November 2018	Yes	
				4	Temporary promotions are not initiated/ceased in accordance with policy	Yvonne Akinmodun, Head of HR	~~October 2018~~ January 2019	Yes	
				5	Failure to identify error and potential fraud	Richard Sydee, Director of Finance and Facilities	~~December 2018~~ Q2 2019/20	No	
				6	Failure to identify and recover overpayments in a timely manner	Yvonne Akinmodun, Head of HR Morounke Akingbola, Head of Finance	September 2018	Yes	
				7	External providers of payroll services operate ineffectively	Yvonne Akinmodun, Head of HR	September 2018	Yes	
			Review of Cyber Security	1	The absence of a defined information security management framework and governance approach, supported by an appropriate high-level risk assessment could lead to the inconsistent treatment of cyber-security and potential security compromises that could have been avoided	Authority Chair/Chair of AGC	March 2019	No	
				4	Ongoing use of ports, protocols and services on networked devices are not managed, increasing the windows of vulnerability available to attackers	Dan Howard, Chief Information Officer	March 2019	No	
				5	The life cycle of system and application accounts is not actively managed, including their creation,	Dan Howard, Chief Information Officer	March 2019 (first review)	Yes	

					use, dormancy and deletion, potentially increasing the number of deliberate and accidental attacks.				
2017/18	Moderate		Data Loss	1	Clinic governance oversight	*Chris Hall, Senior Inspector (Information)*	*Post April 2018*	No	No
				2	Policy Review	*Dan Howard, CIO*	*May 2018*	Yes	Sent 20 Jan-19
				3	Staff Training	*(Dan Howard, CIO & Head of HR)*	*December 2017*	Yes	
			Risk Management	4	Staffing / Capability	*Peter Thompson, CEO (Yvonne Akinmodun, Head of HR)*	*March 2018*	Yes	Sent 20 Jan-19
TOTAL	14								

FINDING/*RISK*	Recommendation	Management Response and agreed actions / Progress update	Owner/Completion date
PAYROLL AND EXPENSES			
2018/19 – INTERNAL AUDIT CYCLE			
1. Inadequate policies and procedures			
Expenses Policy: • Duty of care / Health and Safety regarding employees driving is inadequately addressed within policy. • Inadequate deterrent message regarding the potential for expenses fraud. Insufficient guidance for employees regarding multiple expenses claims	The Expenses Policy will be enhanced to include the following: • Reference to health and safety of employees for driving for prolonged periods and other options to be considered where high mileage claims are to be incurred (for example, Value for Money and options to hire vehicles) • Include reference to the consequences of providing false information i.e. breach of the employee Code of conduct • Provide clear guidance on claiming subsistence for more than one person	Agreed: The Expense policy is to be reviewed in line with changes to flexible working. We will look to make reference to the health and safety of employees however, the Vfm and options we feel is already represented. We will include reference to providing false information and guidance on claiming for more than one person **Sep 18 update**: Expense policy has been re-written and inclusions relating to health and safety, single claimants included.	***Morounke Akingbola, Head of Finance*** ***September 2018*** ***COMPLETE***

FINDING/*RISK*	Recommendation	Management Response and agreed actions / Progress update	Owner/Completion date
PAYROLL AND EXPENSES			
2018/19 – INTERNAL AUDIT CYCLE			
2.	**Incorrect payments to starters and leavers.**		
Use of electronic signatures on employee declarations Declarations on contracts or formal notifications from employees not fully signed / legally binding (if necessary).	HR to seek clarification from HFEA Legal Professionals regarding the acceptability of employee electronic signatures in declarations where emails are present as an audit trail.	Agreed – legal advice to be sought on e-signatures **Sep 18 update:** Based on advice we have been able to obtain - Electronic signatures are considered to be legally binding for employment documents.	***Yvonne Akinmodun, Head of HR*** ***Summer 2018*** **COMPLETE**

FINDING/*RISK*	Recommendation	Management Response and agreed actions / Progress update	Owner/Completion date
PAYROLL AND EXPENSES			
2018/19 – INTERNAL AUDIT CYCLE			
3.	**Inappropriate expense claims paid**		
The Finance Team review of expenses claims. Not all expenses claims are independently checked in the second line of defence stage due to human error.	The Finance Team to review a random sample of expenses on a monthly basis to gain assurances that expenses have been reviewed by members of their team prior to approval (following the revision to the hierarchy) for a minimum period of 3 months, if no concerns are identified.	Agreed (Error was not system generated but human error. Admin rights given to AO have been reviewed and agreement reached regards amendments). Sep 18 update: Review to commence during Q3. Dec-18 update Expense claims reviewed prior to pay-runs by Director of Finance or Head of Finance. Minor issues detected and rectified before payment. This is an on-going process**.**	***Morounke Akingbola, Head of Finance*** ***November 2018*** ***COMPLETE***
Independent, secondary checks of expense claims Line managers approving expenses in the system also undertake reviews of Budget Monitoring reports. In this scenario, the secondary check is not independent.	HFEA Finance Team to investigate the extent to which Budget holders are also approving expenses in the system and consider whether any hierarchy adjustments are required to ensure an independent second line defence is in place	Agreed: We will review the hierarchy of approvals; however, our size and structure will make any changes difficult. Sep 18 update: A review of the hierarchy of approvers was done and we do not feel that any further changes are necessary. Expenses are reviewed by at least 2 separate people.	***September 2018*** **COMPLETE**
Subsistence claims made for multiple employees The associated risks are: • Inability to easily extract full Management Information of expenses claimed per person. • Published expenses data claims may lack clarity / transparency. • Greater risk of duplicate subsistence claims being made where employees are claiming for each other.	Senior Management to review the protocol that enables employees to claim subsistence for more than one person and make an informed decision based on the audit findings of the future approach. The outcome will inform upon the future Expenses Policy review.	Agreed: Incorporated in T&S policy review Sep 18 update: Refreshed T&S policy stipulates that staff must only claim for the own subsistence.	**COMPLETE**

Reputational damage where expenses claims are erroneous.			
FINDING/*RISK*	**Recommendation**	**Management Response and agreed actions / Progress update**	**Owner/Completion date**
PAYROLL AND EXPENSES			
2018/19 – INTERNAL AUDIT CYCLE			
4.	**Temporary promotions are not initiated / ceased in accordance with policy**		
The lack of a formalised process / appropriate sign off is not best practice in terms of transparency, accountability and good governance to ensure decision-making is fair and consistent.	Policy and procedures regarding appointment of temporary promotions will be enhanced to include the following stages: • HR booking milestone reviews of the temporary promotion with the relevant Director. • HR to obtain a decision from the Director / Senior Management regarding whether the appointment will be ceased at a specific date or reviewed at a future date. • The employee will be notified of the decision. • In the event a future end date or review date cannot be determined, HR to review with the Director / Senior Manager at proportionate intervals (no more than annually).	Agreed: We will update our policy on temporary promotions. Sep 18 update: This work is in progress. **Dec 18 update:** We expect to have a draft policy for SMT review by mid-December with dissemination to CMG early January 2019. **March 19 update:** New Pay policy has been drafted which includes section on temporary promotions. Policy shared with CMG via email and to be formerly signed off at March meeting.	***Yvonne Akinmodun, Head of HR*** ***~~October 2018~~*** ***January 2019*** ***COMPLETE***

FINDING/*RISK*	Recommendation	Management Response and agreed actions / Progress update	Owner/Completion date
PAYROLL AND EXPENSES			
2018/19 – INTERNAL AUDIT CYCLE			
5.	**Failing to identify error and potential fraud**		
Management Information / Exception Reporting. Limiting the potential to identify fraud and error and undertake trend analysis regarding expenses.	HFEA to undertake a cost benefit analysis of introducing expenses reporting / duplicate reporting tools within the systems.	Agreed. Sept-18 update: None **Dec-18 update:** A review of systems is underway however; indications are that a wider view needs to be taken with regards the finance, expense and P2P systems. We aim to look into this further in 19/20 business year.	***Richard Sydee, Director of Finance and Facilities*** *~~December 2018~~* ***Q2 2019/20***
Reconciliation of Redfern invoices - Failing to reconcile invoice from Redfern Incorrect billing not identified	Senior Managers issue communications to Budget Holders / Managers to highlight the importance of undertaking the reconciliation of the Redfern Invoice data and to notify the Finance Team when the check is undertaken, even if there are no concerns	Agreed: Communication of importance to be made at CMG and follow-up email to teams Sept 18 update: Raised at CMG July meeting importance of review/sign-off of Redfern invoice. Follow-up email sent post Q2 finance reviews.	***Morounke Akingbola, Head of Finance*** ***July 2018*** **COMPLETE**

FINDING/*RISK*	Recommendation	Management Response and agreed actions / Progress update	Owner/Completion date
PAYROLL AND EXPENSES			
2018/19 – INTERNAL AUDIT CYCLE			
6. Failure to identify and recover overpayments in a timely manner			
Employee overpayments: Under existing arrangements, the associated risks are that in the event of overpayment: a formalised / documented process is not in place to follow that governs treatment of overpayments fairly and consistently. In event of legal challenge on an overpayment, HFEA would be in the strongest position to defend its position if a fair process / policy is in place to support decisions made.	HFEA to introduce a Policy Statement regarding the recovery of overpayments that directly links to overarching Debt Recovery policy.	Agreed HR to draft policy statement on salary overpayments General recovery of monies is detailed in overarching Debt recovery policy. Sept 18 update: HR is in the process of drafting an overpayment policy. We are also updating contracts of employment for future employees that make it clearer what is expected in the event of any overpayments. **Dec 18 update:** New contract of employment templates has been updated to reflect recovery of overpayments. A policy statement will be drafted and shared. **March 19 update:** Policy statement has been included in new Pay Policy which has been shared with CMG for comment.	***Yvonne Akinmodun, Head of HR*** ***~~October 2018~~*** ***January 2019*** ***COMPLETE***
7. External providers of payroll services operate ineffectively			
HFEA have no assurance regarding the strength of controls or stability of systems used by the third party provider of the payroll.	HFEA to examine the contract with FPS to establish whether the supplier is obliged to provide assurance reports, then HFEA to request assurance reports accordingly.	Agreed: Contract will be reviewed, and reports requested. **Sept 18 update:** Our payroll providers have provided us with copies of their GDPR policy. Intermittent reviews of the policy will take place managed by HR to ensure continuing compliance.	***Yvonne Akinmodun, Head of HR*** ***September 2018*** **COMPLETE**

FINDING/*RISK*	Recommendation	Management Response and agreed actions / Progress update	Owner/Completion date
		CYBER SECURITY	
2018/19 – INTERNAL AUDIT CYCLE			
1. The absence of a defined information security management framework and governance approach, supported by an appropriate high-level ris assessment could lead to the inconsistent treatment of cyber-security and potential security compromises that could have been avoided			
HFEA has a defined information security management framework and appropriate structures to support the oversight of the cyber risk. Scrutiny and challenge could be improved further by appointing to the AGC a non-executive member with a background in technology. The management of the cyber security risk should be improved so there is a clear articulation of the controls 'gap' for each element of the cyber risk and necessary steps required to reduce the risk exposure (current score 9) to the desired level (residual risk score 6).	Management should consider appointing a non-executive member to the Audit & Governance Committee who has a background in technology. Management should ensure that the Strategic Risk Register update is improved to clearly articulate details of individual cyber risk element control gaps, the necessary specific mitigating actions, including timelines, to bring cyber risk exposure within tolerance and report these to the next AGC and Authority meetings.	To be considered by AGC **March 19 update**: Discussion or removal? **Dec 18 update**: We have undertaken further cyber security (penetration) testing of the new digital systems such as PRISM and the Register, to ensure that these remain secure. The results have not revealed any significant issues. SMT raised the tolerance level of this risk to 9 in November, reflecting that though we believe our cyber controls are fit for purpose, the context in which we operate, with a high level of national cyber risk, means we are tolerating a higher level of risk. There has been no evidence to suggest the national cyber risk has been further heightened. We continue to assess and review the risk and take action as necessary to ensure our security controls are robust and are working effectively. This strategic risk register has been updated to reflect the above and it will continue to be regularly reviewed as part of our risk monitoring cycle.	***AGC Chair?*** ***March 2019*** ***Dan Howard, Chief Information Office*** ***N/a***

FINDING/*RISK*	Recommendation	Management Response and agreed actions / Progress update	Owner/Completion date
CYBER SECURITY			
2018/19 – INTERNAL AUDIT CYCLE			
5. **The absence of an established security configuration of laptops, servers and workstations using a rigorous configuration management and controls process increase the risk of unauthorised changes to systems, exploitation of unpatched vulnerabilities and insecure system configurations and increases the number of security incidents**			
Aligning more closely with NCSC guidance will help support more robust cyber risk management as will improving discovery and monitoring capability. This is especially important given the confidential nature of information resident in HFEA systems and their acknowledgement that strategic level cyber risk is considered to be outside tolerance.	Management should formally document baselined security configuration standards and develop a process to maintain these on an ongoing basis. Management should develop a software and hardware inventory and integrate this with the protective monitoring capability to help prevent the downloading of unauthorised software by staff and detect instances of unauthorised hardware connecting to the HFEA networks and unauthorised software put onto the HFEA network by external attackers.	Agreed – these will be documented and reviewed on a quarterly basis **March 19 update** Access Management document is complete and will be reviewed at the Information management meeting on 27 February 2019. Network security standards and controls document is underway and will be reviewed at the Information management meeting on 26 March 2019. Agreed: We will create a software inventory of approved software and annually review the results of the software audit to ensure only authorised software is present on the network. No user has administrative permissions by default on HFEA devices which in turn prevents users installing unauthorised software. We use Microsoft Insight to ensure essential security patches are applied as required. **March 19 update** Software inventory is available and is monitored through subscription model (TrustMarque our supplier), network monitoring (Microsoft in Tune) and asset information. This was last reviewed on 25 February 2019 and will be formerly signed off at the Information management meeting on 26 March 2019.	***Dan Howard, Chief Information Officer*** ***1 March 2019*** ***1 January 2019*** ***COMPLETE***

FINDING/*RISK*	Recommendation	Management Response and agreed actions / Progress update	Owner/Completion date
CYBER SECURITY			
2018/19 – INTERNAL AUDIT CYCLE			
6.	**Ongoing use of ports, protocols and services on networked devices are not managed, increasing the windows of vulnerability available to attackers.**		
HFEA has the appropriate directive controls in the form of a comprehensive suite of policies to describe the process and limitations in staff being granted access to systems and services and the associated Role-Based Access Controls. However, we are unclear as to how this is managed in the supply chain.	Management should consider seeking periodic assurances from Azure and Alscient over the management of elevated users, the number with access to HFEA infrastructure, confirmation that the privilege account actions are appropriate and that they cannot see HFEA data or access the systems.	Agreed: This will happen on a quarterly basis. **March 19 update** First review of elevated users ad their activities took place at regular security meeting on 14 February 2019 and is reviewed on a quarterly basis.	***Dan Howard, Chief Information Officer*** ***First review March 2019*** ***COMPLETE***

FINDING/*RISK*	Recommendation	Management Response and agreed actions / Progress update	Owner/Completion date
DATA LOSS			
2018/19 – INTERNAL AUDIT CYCLE			
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 Quality) post will be filled from – Summer 2018* *Nov 17 update:* no update *Feb 18 update:* no update *May 18 update:* The Senior Inspector (Information Quality) will be filled from August 2018 Sept 18 update: The Senior Inspector (Information Quality) will move into his new post later this year (2018). Dec 18 update: The expectation is that the above time frame is still achievable. **March 19 update** This staff move has continued to be delayed pending completion of the PRISM project and data migration The Chief Information Officer and Chief Inspector are continuing to review the impact and to plan for the move in Spring 2019.	***Chris Hall, Senior Inspector (Information Quality)*** ***~~Summer 2018~~*** ***Q3/4 2018/19*** ***Q4 2018***

FINDING/*RISK*	Recommendation	Management Response and agreed actions / Progress update	Owner/Completion date
CYBER SECURITY			
2018/19 – INTERNAL AUDIT CYCLE			
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.* ***Feb 18 update:*** no update ***May 18 update***: The new Acceptable Use Policy was reviewed at CMG on 23 May 18. Final comments will be forward to DH before 6 June 18 and the final version of policy will be reviewed and ratified by CMG on 20 June 2018. **Sept 18 update:** Acceptable Usage policy presented to CMG in June and was approved subject to minor amendments.	***Owner: Dan Howard, CIO*** **May 2018** **COMPLETE**

FINDING/*RISK*	Recommendation	Management Response and agreed actions / Progress update	Owner/Completion date
CYBER SECURITY			
2018/19 – INTERNAL AUDIT CYCLE			
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.* ***Feb 18 update:*** *All staff were required to complete the online IAO training in December 2017. With HR monitoring to ensure completion.* ***Feb 18 update plus*** *HR is also in the process of purchasing a new HRIS, which will enable the training, monitoring and recording of mandatory and other training provided by HFEA.* *It is expected the new system will be in place by early spring 2018* ***May 18 update***: The new HR system is in the process of being configured. It is expected that the new system will go live on 1 July 2018 **Sept 18 update**: People HR went live on 17 September 2018	***Dan Howard, CIO*** ***(Yvonne Akinmodun)*** **December 2017** **COMPLETE** **COMPLETE**

FINDING/*RISK*	Recommendation	Management Response and agreed actions / Progress update	Owner/Completion date
CYBER SECURITY			
2018/19 – INTERNAL AUDIT CYCLE			
4. 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	*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.* ***Feb 18 update:*** Review of staff survey results was conducted in Q3 by CMG and shared with staff in January. Plans are currently being put in place to provide quarterly or bi-annual reports to SMT on the general themes that emerge from exit interviews. Action plans to tackle themes identified from exit interviews will also be put in place ***May 18 update:*** In progress – results from the findings from exit interviews will be reported as part of an annual HR report *Sep 18 update:* Draft exit interview report has been presented to SMT and is now awaiting final sign off ***Dec 18 update:*** Summary Exit interview data shared with CMG in November and AGC to receive as part of bi-annual HR report.	***Peter Thompson, CEO*** ***Yvonne Akinmodun*** ***Before end of 2017*** ***~~End March 2018~~*** **~~October 2018~~** **November 2018** **COMPLETE**
	•Development of a clear workforce strategy that supports management in the recruitment and retention of staff.	Agreed – this is in progress. Finalisation discussion planned at leadership and away day on 29 November 2017. Publication shortly thereafter. **Feb 18 update:** We have a people plan which identified recruitment and retention processes including the review of our induction	

		process to ensure staff feel able to work effectively in as short a period of time as possible. **May 18 update:** A new induction policy and checklist was launched in May 2018. Managers are being offered guidance and support in using the new policy Sep 18 update: HR is organising a lunch and learn session in October for managers to ensure understanding of new policy. **Dec 18 update:** Lunch and Learn session conducted 12 November.	**October 2018** **COMPLETE**

Strategic risk register

Strategic delivery:	☒ Safe, ethical, effective treatment	☒ Consistent outcomes and support	☒ Improving standards through intelligence

Details:	
Meeting	Audit and Governance Committee
Agenda item	15
Paper number	AGC (05/03/2019) 665 HC
Meeting date	5 March 2019
Author	Helen Crutcher, Risk and Business Planning Manager
Output:	
For information or decision?	For 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. SMT review the strategic risk register monthly. AGC reviews the strategic risk register at every meeting. The Authority reviews the strategic risk register periodically (at least twice per year).
Communication(s)	Feedback from AGC will inform the next SMT review in March. Authority is due to receive the register in May.
Organisational risk	□ Low ☒ Medium □ High
Annexes	Annex 1: Strategic risk register

1. Latest reviews

1.1. SMT reviewed the register at its meeting on 28 January. SMT reviewed all risks, controls and scores.

1.2. Authority and SMT’s comments are summarised in the commentary for each risk and at the end of the register, which is attached at Annex A. The annex also includes a graphical overview of residual risk scores plotted against risk tolerances.

1.3. None of the six risks are above tolerance.

2. Recommendation

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

Latest review date – 18/02/2019

Strategic risk register 2018/19

Risk summary: high to low residual risks

Risk area	Strategy link*	Residual risk	Status	Trend**
C1: Capability	Generic risk – whole strategy	**12 – High**	At tolerance	⬄⬄⬄⬄
CS1: Cyber security	Generic risk – whole strategy	**9 – Medium**	At tolerance	⬄⬄⬄⬄
LC1: Legal challenge	Generic risk – whole strategy	**8 – Medium**	Below 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	⬄⬄⬄⬄
FV1: Financial viability	Generic risk – whole strategy	**6 – Medium**	Below 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, SMT or the Authority (eg,⇧⬄⇩⬄).

Recent review points are: Authority 14 November ⇨ SMT 19 November ⇨ AGC 4 December ⇨ SMT 28 January

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**
3	4	12 - High	**2**	**3**	**6 - 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
Below tolerance. Indications to date are that income is in line with the predictive income model and there has been a small increase in treatment cycles from last year; this risk is therefore stable. We have reviewed budgets at the end of Q3 forecast an underspend on our legal budget, following the resolution of a pending appeal in October. CMG considered options for the effective reallocation of this money, to achieve the maximum strategic benefit and approved several proposals, to be completed before April. We still project an underspend at year end.

Causes / sources	Mitigations	Timescale / owner
There is uncertainty about the annual recovery of treatment fee income – this may not cover our annual spending.	Heads see quarterly finance figures and would consider what work to deprioritise or reduce should income fall below projected expenditure. We have a model for forecasting treatment fee income and this reduces the risk of significant variance, by utilising historic data and future population projections. We will refresh this model quarterly internally and review at least annually with AGC.	Quarterly, ongoing, with AGC model review at least annually - next review due in 2019 - Richard Sydee

Our monthly income can vary significantly as: - it is linked directly to level of treatment activity in licensed establishments - we rely on our data submission system to notify us of billable cycles.	Our reserves policy takes account of monthly fluctuations in treatment activity and we have sufficient cash reserves to function normally for a period of two months if there was a steep drop-off in activity. The reserves policy was reviewed by AGC in December 2018. If clinics were not able to submit data and could not be invoiced for more than three months we would invoice them on historic treatment volumes and reconcile this against actual volumes once the submission issue was resolved and data could be submitted.	Ongoing – Richard Sydee In place – 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 flag any shortfall or further funding requirements. All project business cases are approved through CMG, so any financial consequences of approving work are discussed.	Quarterly meetings (on-going) – Morounke Akingbola Ongoing – Richard Sydee
Inadequate decision-making leads to incorrect financial forecasting and insufficient budget.	Within the finance team there are a series of formalised checks and reviews, including root and branch analyses of financial models and calculations. The organisation plans effectively to ensure enough time and senior resource for assessing core budget assumptions and subsequent decision making.	In place and ongoing - Richard Sydee Quarterly meetings (on-going) – Morounke Akingbola
Project scope creep leads to increases in costs beyond the levels that have been approved.	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. Any exceptions to tolerances are discussed at Programme Board and escalated to CMG at monthly meetings, or sooner, via SMT, if the impact is significant or time-critical.	Ongoing – Richard Sydee or Morounke Akingbola Monthly (on-going) – Morounke Akingbola
Failure to comply with Treasury and DHSC spending controls and finance policies and guidance leads to serious reputational risk and a loss of financial autonomy or goodwill for securing future funding.	The oversight and understanding of the finance team ensures that we do not inadvertently break any rules. The team's professional development is ongoing and this includes engaging and networking with the wider government finance community. All HFEA finance policies and guidance are compliant with wider government rules. Policies are reviewed annually, or before this if required. Internal oversight of expenditure and approvals provides further assurance (see above mitigations).	Continuous - Richard Sydee Annually and as required – Morounke Akingbola
Risk interdependencies	**Control arrangements**	**Owner**

(ALBs / DHSC)		
DHSC: Legal costs materially exceed annual budget because of unforeseen litigation.	Use of reserves, up to contingency level available. The final contingency for all our financial risks would be to seek additional cash and/or funding from the Department.	Monthly – Morounke Akingbola
DHSC: GIA funding could be reduced due to changes in Government/policy.	A good relationship with DHSC Sponsors, who are well informed about our work and our funding model.	Accountability quarterly meetings (on-going) – Richard Sydee
	Annual budget agreed with DHSC Finance team alongside draft business plan submission. GIA funding has been provisionally agreed through to 2020.	December/January annually – Richard Sydee

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**
4	4	16 – High	**4**	**3**	**12- 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

At 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.

Turnover remains high. Evidence suggests that the two main drivers of high turnover are the continuing constraints on public sector pay and the relatively few development opportunities in small organisations like the HFEA. Consequently, we are carrying a handful of vacancies, and in some areas, there is a trend towards over-reliance on key individuals. The position is particularly acute in the Compliance and Information directorate.

Work continues to improve the offer to staff, with the aim of increasing the likelihood of staff staying in post and developing at the HFEA, rather than leaving, although we are limited by a small organisation with little room to offer opportunities for promotion and wider government pay constraints. Elements of this include the PerkBox benefits scheme for staff, buying and selling of annual leave policy and ongoing cultural change work.

Following the 2018 staff survey and the December 2018 staff awayday, an action plan has been shared with staff and this will be reviewed on a regular basis to ensure that progress continues.

AGC received a paper on HR data in December 2018, to consider the situation in the round, including ongoing strategies for the handling of these risks, and further updates will be provided to allow them to track progress. Looking further ahead, we need to find ways to tackle the issues of pay and development opportunities, to prevent this risk increasing further. An idea we are keen to explore is whether we can build informal links or networks with other public sector or health bodies, to develop clearer career paths between organisations.

Causes / sources	Mitigations	Timescale / owner

High turnover, sick leave etc., leading to temporary knowledge loss and capability gaps.	Organisational knowledge captured via documentation, handovers and induction notes, and manager engagement. We have developed corporate guidance for all staff for handovers. A checklist for handovers is circulated to managers when staff hand in their notice. This checklist will reduce the risk of variable handover provision.	In place – Yvonne Akinmodun Checklist in use – Yvonne Akinmodun
	Vacancies are addressed speedily, and any needed changes to ways of working or backfill arrangements receive immediate attention. CMG and managers prioritise work appropriately when workload peaks arise.	In place – Yvonne Akinmodun In place – Peter Thompson
Poor morale could lead to decreased effectiveness and performance failures.	Communication between managers and staff at regular team and one-to-one meetings allows any morale issues to be identified early and provides an opportunity to determine actions to be taken. The new intranet, which launched in October 2018 has enabled more regular internal communications.	In place, ongoing – Peter Thompson In place – Jo Triggs
	Work continues to implement actions in the people plan which launched in April 2018 and reflected staff feedback. Further actions have been identified through the 2018 staff survey and awayday. An action plan is in place from January 2019 and will be regularly reviewed to ensure that actions are effective. In 2018 new benefit options were implemented, including PerkBox and a buying and selling of annual leave policy (launched July 2018).	Annual survey and staff conferences – Yvonne Akinmodun In place - Peter Thompson
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 at monthly meetings.	In place – Paula Robinson
	Oversight of projects by both the monthly Programme Board and CMG meetings, to ensure that projects end through due process (or closed, if necessary). We are re-launching our interdependencies matrix in early 2019, which supports the early identification of interdependencies in projects and other work, to allow for effective planning of resources.	In place – Paula Robinson Matrix relaunching early 2019 – 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 – further work to be done in 2018/19 -

		Paula Robinson
	Team-level service delivery planning for the next business year, with active involvement of team members. CMG will continue to review planning and delivery. Requirement for this to be in place for each business year.	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 Winter 2018/19 – Dan Howard
Future increase in capacity and capability needed to process and assess licensing activity including mitochondrial donation applications. Since Summer 2017, we have experienced resource pressures relating to the Statutory Approvals Committee, caused in part by mitochondrial donation applications and also the increasing complexity and volume of PGD conditions.	Licensing processes for mitochondrial donation are in place (decision trees etc). An external review of the HFEA licensing processes was carried out to assess current capabilities and processes and make changes for the future. We are in the process of implementing the relevant proposals. As part of this, recruitment is underway within the governance team, to support the licensing function and ensure our committees are supported effectively. To mitigate the present capacity and capability issues, the executive has signed up more experienced mitochondria peer reviewers, have received feedback on the process and have made administrative changes to improve it. This includes improvements to the application form, to prevent additional administration and/or unnecessary adjournments.+	Licensing review implementation underway from September 2018 – Paula Robinson / Clare Ettinghausen
Implementing the People Plan to maximise organisational capability 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.	A leadership awayday in November 2017 and an all staff awayday in January 2018 focused on building an HFEA culture following organisational changes. Small focus groups have since been utilised to make the most of staff time and involve wider staff in developing proposals. The staff away day in December 2018 produced further proposals, to be implemented through an ongoing action plan from January 2019.	Ongoing – Yvonne Akinmodun
Following organisational change implementation and a period of churn, a number of staff are simultaneously 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 are provided where required. Knowledge management via records management and documentation and the HR team has revised onboarding methods to make them clearer and more effective.	In progress – Peter Thompson In place – Yvonne Akinmodun

The future office move, occurring in 2020, may not meet the needs of staff (for instance location), meaning staff decide to leave sooner than this, leading to a significant spike in turnover, resulting in capability gaps.	We will consult with staff, to ensure that their needs are taken into account, where possible, when planning for the move. We plan to explore possible knowledge and capability benefits arising from the office move, such as the potential to open up closer working and career progression with other health regulators.	Early engagement with staff and other organisations underway and ongoing – Richard Sydee
The new organisational model may not achieve the desired benefits for organisational capability Delay in completing our digital projects means that elements of the new model have not been fully implemented. It will therefore take more time for us to validate whether the changes have been effective.	The model will be kept under review following implementation to ensure it yields the intended benefits. The staff survey provided an opportunity for staff to reflect on whether change has been well managed. The results will help to inform any further actions related to the model.	A review of the new model was presented to AGC in June 2018. Staff survey in October 2018 – Peter Thompson
Risk interdependencies **(ALBs / DHSC)**	**Control arrangements**	**Owner**
Government/DHSC: 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 in the past eg, the Triennial Review in 2016.	In place – Peter Thompson
Government/DHSC The UK leaving the EU may have unexpected operational consequences for the HFEA which divert resource and threaten our ability to deliver our strategic aims.	The department has provided guidance about the impact of a no-deal EU exit on the import of gametes and embryos. We continue to work closely to ensure that we are prepared and can provide detailed guidance to the sector at the earliest opportunity, to limit any impact on patients. We have provided ongoing updates to the sector. In December 2018, we commenced an EU exit project to ensure that we fully consider implications and are able to build enough knowledge and capability to handle the effects of the UK's exit from the EU, as a third country in relation to import and export of gametes. This project includes our role in communicating with the sector on the effects of EU exit, to ensure that clinics are adequately prepared in terms of staffing and access to equipment and materials to continue to provide high quality and safe care to patients.	Communications ongoing – Peter Thompson

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**	**3**	**9 - Medium**
Tolerance threshold:					**9 - Medium**

Risk area	Risk owner	Links to which strategic objectives?	Trend
Cyber security CS1: Security and infrastructure weaknesses	Peter Thomson, Chief Executive (pending start of new Director of Compliance and Information)	Whole strategy	⇔⇔⇔⇔

Commentary

Above tolerance.

We have undertaken further cyber security (penetration) testing of the new digital systems such as PRISM and the Register, to ensure that these remain secure. The results have not revealed any significant issues. The third and final test is scheduled ahead of go-live.

We continue to assess and review the level of national cyber security risk and take action as necessary to ensure our security controls are robust and are working effectively. The results of a cyber security audit were received in December 2018, the rating of this audit was moderate with no significant weaknesses found.

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 reports at each meeting on cyber-security and associated internal audit reports. The Vice Chair of the Authority is regularly appraised on actual and perceived cyber risks. Internal audit report on data loss (October 2017) gave a 'moderate' rating, recommendations have been actioned, one final recommendation is being reported at each AGC meeting. A further cyber security internal audit report was finalised in December 2018. A final report on cyber security will be signed off by AGC before any decision is made to go live with PRISM.	Ongoing regular reporting – Director of Compliance and Information/ Dan Howard Ongoing – Dan Howard To occur Winter 2018/19

Changes to the digital estate open up potential attack surfaces or new vulnerabilities. Our relationship with clinics is more digital, and patient identifying information or clinic data could therefore be exposed to attack.	The website and Clinic Portal are secure and we have been assured of this. The focus now is on obtaining similar assurance through penetration testing report to the SIRO in relation to the remaining data submission deliverables (PRISM). The second of three rounds of penetration testing has been completed and there have been no significant issues found so far.	Penetration testing underway throughout development and ongoing – Peter Thompson/ Dan Howard
There is a risk that IT demand could outstrip supply meaning IT support doesn't meet the business requirements of the organisation and so we cannot identify or resolve problems in a timely fashion. We do not currently have a developer in post.	We continually refine the IT support functional model in line with industry standards (ie, ITIL). We undertook an assessment of our ticketing systems and launched a new system in November 2018. Following implementation, we will introduce ways to capture user feedback. Following the completion of an earlier short-term cover arrangement, we have agreed to engage the third-party supplier again to provide further short-term cover, from November 2018 for a period of 4/5 months. We will look to recruit to an in-house software development team following a workload review to take place jointly with the external supplier. Limited external support is likely to be needed for the in-house team on a permanent ongoing basis and this will be explored in due course	Approved per the ongoing business plan – Dan Howard Short-term arrangement in place from November 2018 for 4/5 months. Longer-term discussions underway – Dan Howard
Confidentiality breach of Register or other sensitive data by HFEA staff.	Staff are made aware on induction of the legal requirements relating to Register data. All staff have annual compulsory security training to guard against breaches of confidentiality although we are now due to refresh this. Relevant and current policies to support staff in ensuring high standards of information security. There are secure working arrangements for all staff both in the office and when working at home (end to end data encryption via the internet, hardware encryption) Further to these mitigations, any malicious actions would be a criminal act.	In place – Peter Thompson A review of current IT policies is underway and due for completion by summer 2019 – Dan Howard
There is a risk that technical or system weaknesses lead to loss of, or inability to access, sensitive data, including the Register.	Back-ups of the data held in the warehouse in place to minimise the risk of data loss. Regular monitoring takes place to ensure our data backup regime and controls are effective. We are ensuring that a thorough investigation takes place prior, during, and after moving the Register to the Cloud. This involves the use of third party experts to design and implement the configuration of new architecture, with security and reliability factors considered.	In place – Dan Howard Results of penetration testing have been positive. The new Register will be in use from Winter

		2018/19 – Dan Howard
Business continuity issue (whether caused by cyber-attack, internal malicious damage to infrastructure 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. A plan is in place for the next Business Continuity test. Existing controls are through secure off-site back-ups via third party supplier. A cloud backup environment has been set up to provide a further secure point of recovery for data which would be held by the organisation. The cloud backup environment for the new register has been successfully tested. Once the final penetration tests are complete we will utilise this functionality as we go live with our new register and submission system.	BCP in place, regularly tested and reviewed – Director of Compliance & Information/ Dan Howard Undertaken monthly – Dan Howard The new Register cloud backup environment will come into use in Winter 2018/19 - Dan Howard
The corporate records management system (TRIM) is unsupported and unstable and we are carrying an increased risk of it failing. The organisation may be at risk of poor records management until the new system is functioning and records successfully transferred.	A formal project to replace our electronic document management system is underway, for delivery of a new system in 2019. We are continuing to manage the existing risk with the TRIM system by minimising changes and monitoring performance regularly. All staff have been reminded to continue to use TRIM to ensure records are complete.	Project to be delivered in 2019 – Dan Howard
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 – Dan Howard
Risk interdependencies (ALBs / DHSC)	**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 given the ethically contested and legally complex issues it regulates.

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	5	20 – Very high	**2**	**4**	**8 - Medium**
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
Below tolerance. We accept that in a contested area of public policy, the HFEA and its decision-making will be legally challenged. Legal challenge poses two key threats: • that resources are substantially diverted • that the HFEA's reputation is negatively impacted by our participation in litigation. These may each affect our ability to regulate effectively and deliver our strategy. Both the likelihood and impact of legal challenge may be reduced, but it cannot be avoided entirely. For these reasons, our tolerance for legal risk is high.

Causes / sources	**Mitigations**	**Timescale / owner**
Assisted reproduction is complex and controversial and the Act and regulations are not beyond interpretation. This may result in challenges to the way the HFEA has interpreted and applied the law.	Evidence-based and transparent policy-making and horizon scanning processes. Horizon scanning meetings occur with the Scientific and Clinical Advances Advisory Committee on an annual basis.	In place – Laura Riley with appropriate input from Catherine Drennan
	Through constructive engagement with third parties, the in-house legal function serves to anticipate issues of this sort and prevent challenges or minimise the impact of them. Where necessary, we can draw on the expertise of an established panel of legal advisors, whose experience across other sectors can be applied to put the HFEA in the best possible position to defend any challenge.	Ongoing – Catherine Drennan In place – Peter Thompson

	Case by case decisions on the strategic handling of contentious issues in order to reduce the risk of challenge or, in the event of challenge, to put the HFEA in the strongest legal position.	In place – Catherine Drennan and Peter Thompson
	We undertake good record keeping, to allow us to identify and access old versions of guidance, and other key documentation, which may be relevant to cases or enquiries and enable us to see how we have historically interpreted the law.	In place – Catherine Drennan
Committee decisions or our decision-making processes may be contested. ie, Licensing appeals and/or JRs.	Panel of legal advisors in place to advise committees on questions of law and to help achieve consistency of decision-making processes. The Head of Legal has put measures in place to ensure consistency of advice between the legal advisors from different firms. These include: • Provision of previous committee papers and minutes to the advisor for the following meeting • Annual workshop (next due April 2019) • A SharePoint site for sharing questions, information and experiences is in development	In place – Peter Thompson Since Spring 2018 and ongoing – Catherine Drennan
	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 February 2019). Project underway to implement changes in the light of the findings of an external licensing review, to make the licensing process more efficient and robust.	In place, further development underway as part of the licensing review implementation project – Paula Robinson
	Well-evidenced recommendations in inspection reports mean that licensing decisions are adequately supported and defensible.	In place – Sharon Fensome-Rimmer
High-profile legal challenges have reputational consequences for the HFEA which risk undermining the robustness of the regulatory regime and affecting strategic delivery.	Close working between legal and communications teams to ensure that the constraints of the law and any HFEA decisions are effectively explained to the press and the public. The default HFEA position is to conduct litigation in a way which is not confrontational, personal or aggressive.	In place – Catherine Drennan, Joanne Triggs In place – Peter Thompson, Catherine Drennan

	The Compliance team stay in close communication with the Head of Legal to ensure that it is clear if legal involvement is required, to allow for effective planning of work. The Compliance management team monitor the number and complexity of management reviews to ensure that the Head of Legal is only involved as appropriate.	In place – Sharon Fensome Rimmer, Director of Compliance & Information
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 significant 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 – Clare Ettinghausen
The Courts approach matters on a case by case basis and therefore outcomes can't always be predicted. So, the extent of costs and other resource demands resulting from a case can't necessarily be anticipated.	Scenario planning is undertaken with input from legal advisors at the start of any legal challenge. This allows the HFEA to anticipate a range of different potential outcomes and plan resources accordingly.	In place – Peter Thompson
Legal proceedings can be lengthy and resource draining and divert the in-house legal function (and potentially other colleagues) away from business as usual.	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 workload should this become necessary.	In place – Peter Thompson
HFEA process failings could create or contribute to legal challenges, or weaken cases that are otherwise sound,	Licensing SOPs were improved and updated in Q1 2018/19, committee decision trees in place. Advice sought through the Licensing review on specific legal points, so that improvements can be identified and implemented. A project to implement these is underway.	In place – Paula Robinson From October 2018 – Paula Robinson
	Up to date compliance and enforcement policy and related procedures to ensure that the Compliance team acts consistently according to agreed processes.	In place but in the process of being reviewed Q4 2018/19 – Catherine Drennan
Legal parenthood consent cases are ongoing and some are the result of more recent	The Head of Legal continues to keep all new cases under review, highlighting any new or unresolved compliance issues so that the	In progress and ongoing – Catherine

failures (the mistakes occurred within the last year). This may give rise to questions about the adequacy of our response when legal parenthood first emerged as a problem in the sector (in 2015).	Compliance team can resolve these with the clinic(s).	Drennan, Sharon Fensome-Rimmer, Director of Compliance & Information
Storage consent failings at clinics are leading to a significant diversion of legal resource and additional costs for external legal advice.	We have taken advice from a leading barrister on the possible options for a standard approach for similar cases. We are in the process of considering how the advice can be interpreted in guidance which can be applied broadly across the sector. The Head of Legal made significant amendments to guidance in the Code of Practice dealing with consent to storage and extension of storage. This guidance should mean that clinics are clearer about their statutory responsibilities and thus prevent issues arising in the future.	Done in Q1 2018/19 – Catherine Drennan Revised version of the Code launched January 2019 – Laura Riley
GDPR requirements require a large number of changes to practice. If we fail to comply with the requirements, this could open the HFEA up to legal challenge and possible fines from the Information commissioner's office.	The GDPR project introduced a number of new and updated policies and processes, to ensure that the HFEA complies with the requirements. These will now be bedded into BAU to ensure that they are effective. The project was handled proactively, with a joint HFEA and HTA project team and sponsored directly by the Director of Finance and Resources to ensure senior oversight. Although the project was closed in October, ongoing actions are being closely monitored to ensure effective compliance. AGC have regular updates on progress.	Ongoing- Richard Sydee
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
DHSC: 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 and Social Care 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 DHSC would be involved in resolving it.	In place – Peter Thompson
DHSC: 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.	In place – Peter Thompson

	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	

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 - High	**2**	**3**	**6 – Medium**
Tolerance threshold:					**6 - Medium**

Risk area	Risk owner	Links to which strategic objectives?	Trend
Regulatory effectiveness RE 1: Inability to translate data into quality	Peter Thomson, Chief Executive (pending start of new Director of Compliance & 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. Data submission work continues although delivery has been somewhat delayed owing to complexities. Delivery should be during winter 2018/19.

Causes / sources	Mitigations	Timescale / owner
IfQ has taken longer than planned, and there will be some ongoing development work needed leading to delays in accessing the benefits.	Data Submission development work is now largely complete, with clinic implementation and access to it following by Winter 2018/19. Oversight and prioritisation of any remaining development work will be through the IT development programme board.	Completion of data submission project Winter 2018/19 – Director of Compliance & Information
Risks associated with data migration to new structure, compromises record accuracy and data integrity.	Migration of the Register is highly complex. IfQ programme groundwork focused on current state of Register. There is substantial high-level oversight including an agreed migration strategy which is being followed. The migration will not go ahead until agreed data quality thresholds are met. AGC will have final sign off on the migration.	Winter 2018/19, with regular reporting on progress prior to this – Director of Compliance & Information /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. Further scoping work would occur periodically to review whether any additions were needed. The structure of the new Register makes adding additional fields more straightforward than at present.	In place regular reviews to occur once the Register goes live – Director of Compliance & Information
Risk that existing infrastructure systems – (eg, Register, EDI, network, backups) which will be used to access the improved data and intelligence are unreliable.	Maintenance of desktop, network, backups, etc. core part of IT business as usual delivery. In March 2018 CMG agreed to a new approach, including some outsourcing of technical second and third line support, this provides greater resilience against unforeseen issues or incidents. As noted above under CS1, we have a further temporary arrangement in place for ongoing external support for 4/5 months from November 2018 and are considering ongoing requirements.	In place – Dan Howard
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. Two vacancies in the inspection team were filled in November 2018 and there will be a period of bedding in now that they have joined. Recruitment for one vacancy is underway.	In place – Director of Compliance & Information
Failure to integrate the new data and intelligence systems into Compliance activities due to cultural silos.	Work is underway in 2018 to further define and bed in HFEA culture in the light of organisational changes. The people plan was agreed in spring 2018.	Ongoing - Yvonne Akinmodun
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 data submission project. Plan in place to deal with any inability to supply data. The Compliance management team are considering how to manage any centres with EPRS systems who are not ready to provide Register data in the required timeframe. This may include regulatory sanctions. Early engagement with EPRS providers means the risk of non-compliance is slim.	Ongoing - Director of Compliance & Information
Data migration efforts are being privileged over data quality leading to an increase in outstanding errors	The Register team uses a triage system to deal with clinic queries systematically, addressing the most critical errors first.	In place – Director of Compliance & Information

	We undertake an audit programme to check information provision and accuracy. The minimum National Audit Office required audits have been delivered, several further audits have been planned for completion before the years' end.	In place – Director of Compliance & Information
Excessive demand on systems and over-reliance on a few key expert individuals – request overload – leading to errors	PQs and FOIs have dedicated expert staff to deal with them although they are very reliant on a small-number of individuals. We have systems for checking consistency of answers.	In place – Clare Ettinghausen
	There is a dedicated team for responding to OTRs and all processes are documented to ensure information is provided consistently	In place – Dan Howard
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.	The intelligence strategy focuses in part on making the best use of the information gleaned from patients, and converting our mix of soft and hard data into real outcomes and improvements. This includes a new patient survey we piloted in 2018 to give us qualitative and quantitative data on patient's experience of fertility treatment in the UK. The findings of this survey were published in January 2019.	Plan to be developed following the pilot patient survey – Clare Ettinghausen/ Head of Intelligence/Jo Triggs
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
None	-	-

ME1: There is a risk that patients and our other stakeholders do not receive the right information and guidance from us.

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	Clare Ettinghausen 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. We are in the process of revisiting our wider communications strategy to ensure that it remains fit for purpose, this was presented to the Authority in January 2019.

Causes / sources	Mitigations	Timescale / owner
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.	When there are messages that need to be conveyed to clinics through the inspection team, staff work with the team so that a co-ordinated approach is achieved and messages that go out to the sector through other channels (eg clinic focus) are reinforced. When there are new or important issues or risks that may impact patient safety, alerts are produced collaboratively by the Inspection, Policy and Communications teams.	In place - Sharon Fensome-Rimmer, Laura Riley, and Jo Triggs
Patients and other stakeholders do not receive the correct guidance or information.	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 and reviewed periodically (review underway Jan 2019) – Jo Triggs

	The new publication schedule uses HFEA data more fully and makes this more accessible. Policy team ensures guidance is created with appropriate stakeholder engagement and is developed and implemented carefully to ensure it is correct. Ongoing user testing and feedback on information on the website allows us to properly understand user needs. We have internal processes in place which meet The Information Standard. Authority agreed new option for the Donor Conceived register in January 2019. Plans are in place to procure new providers before 31 March 2019. The executive is actively considering interim arrangements should the new supplier be unable to start from 1 April 2019.	Ongoing – Head of Intelligence In place – Laura Riley, Jo Triggs In place –Jo Triggs Certification in place, although the assessment and certification scheme is being phased out – Jo Triggs Interim arrangement in place and ongoing plans being considered – Peter Thompson
We are not able to reach the right people with the right message at the right time.	We have an ongoing partnership with NHS.UK to get information to patients early in their fertility journey and signpost them to HFEA guidance and information. Planning for campaigns and projects includes consideration of communications channels. When developing policies, we ensure that we have strong communication plans in place to reach the appropriate stakeholders. Extended use of social media to get to the right audiences. The communications team analyse the effectiveness of our communications channels at Digital Communications Board meetings, to ensure that they continue to meet our user needs.	In place – Jo Triggs In place and ongoing – Jo Triggs In place - Laura Riley, Jo Triggs In place– Jo Triggs Ongoing – Jo Triggs
Risk that incorrect information is provided in PQs, OTRs or FOIs and this may lead to misinformation and misunderstanding by patients, journalists and others.	PQs and FOIs have dedicated expert staff to manage them. We have systems for checking consistency of answers and a member of SMT must sign off every PQ response before submission.	In place - Clare Ettinghausen Clare Ettinghausen /SMT - In place

	There is a dedicated OTR team and all responses are checked before they are sent out to applicants to ensure that the information is accurate.	In place - Dan Howard
Some information will be derived from data, so depends on risk above being controlled.	See controls listed in RE1, above.	
There is a risk that we provide inaccurate information and data on our website or elsewhere.	All staff ensure that public information reflects the latest knowledge held by the organisation.	In place - Head of Intelligence, Laura Riley, and Jo Triggs
	The Communications team work quickly to amend any factual inaccuracies identified on the website.	In place – Jo Triggs
	The Communications publication schedule includes a review of the website, to update relevant statistics when more current information is available.	In place – Jo Triggs
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
NHS.UK: The NHS website and our site contain links to one another which could break	We maintain a relationship with the NHS.UK team to ensure that links are effectively maintained.	In place – Jo Triggs
DHSC: interdependent communication requirements may not be considered	DHSC and HFEA have a framework agreement for public communications to support effective co-operation, co-ordination and collaboration and we adhere to this.	In place – Jo Triggs

Reviews and revisions

SMT review – January 2019 (28/01/19)

SMT reviewed all risks, commentary, controls and scores and made the following detailed points:

- CS1 – SMT noted that various controls needed updating and that a review of this risk would therefore be done following the meeting with the Chief Information Officer.
- EU Exit – SMT noted that the Director of Strategy and Corporate Affairs would be the main contact on this once the Director of Compliance and Information leaves the organisation. The Chief Executive remained the overall risk owner.
- SMT agreed that the Chief Executive would be the overall risk owner for the strategic risks owned by the Director of Compliance and Information following the departure of Nick Jones and until his successor started.

AGC review – December 2018 (04/12/18)

AGC reviewed the risk register and scores and did not change any of these. The committee made the following points in discussion:

- CS1 - Members discussed cyber security and one asked whether there was a chance we were being complacent with the medium residual rating of this risk. The committee noted that the risk had been reviewed in the light of wider system-wide cyber risks and that the CIO was satisfied. The committee heard that compared to the rest of the health system, we were well placed in terms of cyber security.

- AGC asked about business continuity arrangements and a plan for handling situations of civil unrest. Members heard that the plan was about to be tested and that this scenario could be reviewed as part of this.
- C1 - AGC discussed risks around estates. The move was being planned by a central project group and plans were becoming clearer. A subsequent internal move project would be initiated in 2019 once the broad business case had been agreed by the department. Key concerns would be internal communications, logistics and change management. A member noted that the move brought with it opportunities, particularly in relation to addressing staffing risks by enabling us to make connections with other organisations and create career paths. Members noted that as the situation developed this risk would be fleshed out and it may be appropriate for this to become a new strategic risk area once the shape of developments was clearer.
- AGC discussed the UK's exit from the EU and how this was reflected on the risk register. The department gave an update on the preparations for a no-deal scenario. Until a deal was agreed by EU member state parliaments these preparations would continue. The Chief Executive noted that the main concern for the sector would be access to replacement equipment and medication if these were sourced from overseas. The committee noted that the Director of Compliance and Information would be the key contact with the department on the UK's exit from the EU.

SMT review – November 2018 (19/11/18)

SMT reviewed all risks, commentary, controls and scores and made the following detailed points:

- CS1 – SMT discussed business continuity arrangements and plans. SMT noted that a plan was not yet in place for the next business continuity test, a test had not occurred since September 2017. SMT agreed that a check of staff contact details should occur and the business continuity plan should be circulated to ensure all staff were clear about roles and responsibilities. This was particularly important given the number of new starters. A test should follow. The timing was expedient as a business continuity audit was underway.
- SMT had a full discussion about the tolerance level for the cyber risk, noting that we had reported this as above tolerance since July. Every care was continuing to be taken around data security and SMT were satisfied the controls were effective. However, as had been acknowledged when SMT raised the residual risk level in July, the context in which the organisation was operating was inherently riskier. SMT therefore agreed that we were not 'above tolerance' for this risk, but our tolerance level had increased somewhat. SMT agreed that the risk should have a tolerance of 9.
- RE1- SMT discussed the effect of current resource pressures on the delivery of the audit programme. The minimum number of audits required by the National Audit Office had already been delivered, however further audits that were due to be scheduled at the outset of the year had not been undertaken due to lack of resource in the Register team. The Director of Compliance noted that he was discussing this with the new Register Team Leader to ensure that further audits were planned and enable a greater level of control and assurance.
- Updates had been done throughout to reflect the delayed delivery of the data submission and migration projects.

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	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		1. Rare (≤10%)	2. Unlikely (11%-33%)	3. Possible (34%-67%)	4. Likely (68%-89%)	5. Almost Certain (≥90%)
		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 interdependencies in collaboration with relevant other bodies, and so that we can report easily and transparently on such interdependencies to DHSC or auditors as required.

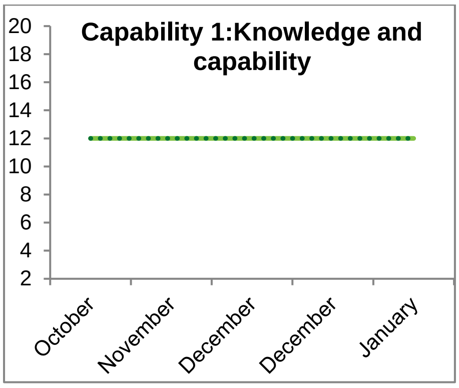
Contingency actions

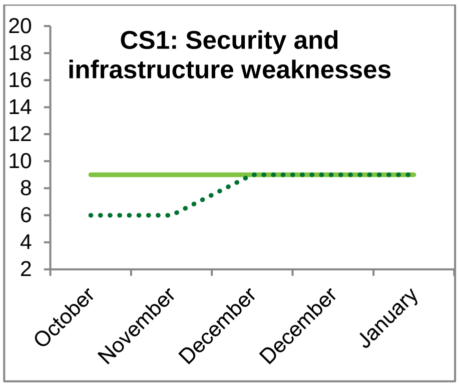
When putting mitigations in place to ensure that the risk stays within the established tolerance threshold, the organisation must achieve balance between the costs and resources involved in limiting the risk, compared to the cost of the risk translating into an issue. In some circumstances it may be possible to have contingency plans in case mitigations fail, or, if a risk goes over tolerance it may be necessary to consider additional controls.

When a risk exceeds its tolerance threshold, or when the risk translates into a live issue, we will discuss and agree further mitigations to be taken in the form of an action plan. This should be done at the relevant managerial level and may be escalated if appropriate.

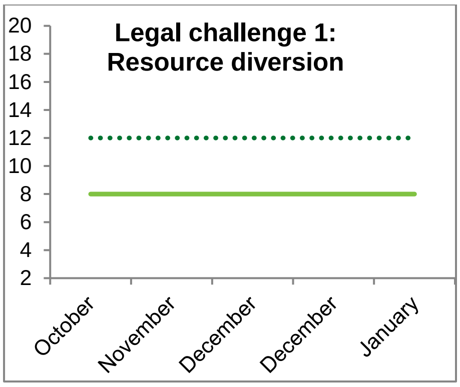
Risk trends

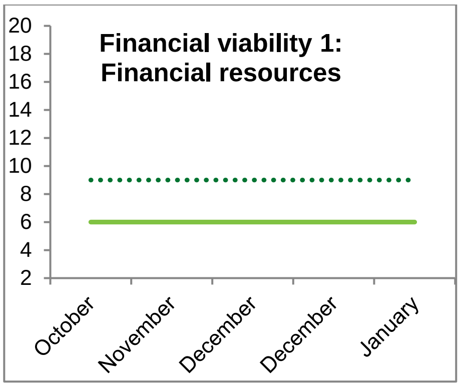
High and above tolerance risks

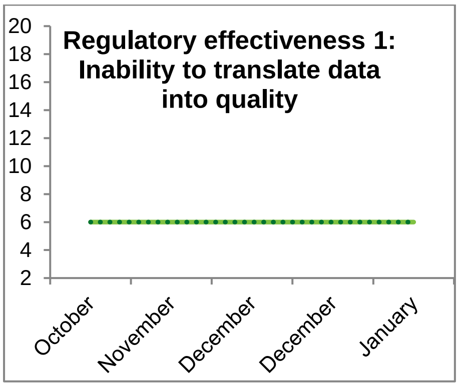


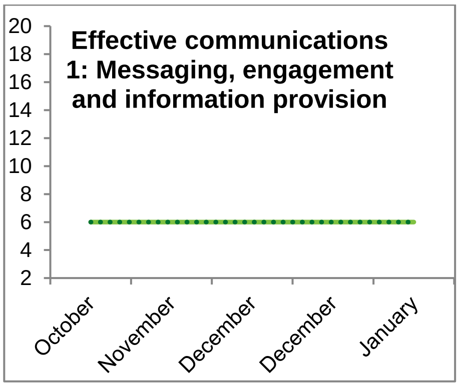


Low and below tolerance risks









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	16		
Paper number	AGC (04/12/2018) 666		
Meeting date	4 December 2018		
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. The Committee are asked to agree to add Draft Annual Governance Statement to the March meetings		
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:	5 Mar 2019	18 Jun 2019	8 Oct 2019	3 Dec 2019
Following Authority Date:	**13 Mar 2019**	**3 July 2019**	**13 Nov 2019**	**Jan 2020**
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
Digital Programme Update	Yes	Yes	Yes	Yes
Annual Report & Accounts (inc Annual Governance Statement)	Draft 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:	5 Mar 2019	18 Jun 2019	8 Oct 2019	3 Dec 2019
HR, People Planning & Processes		Yes Including bi-annual HR report		Bi-annual HR report
Strategy & Corporate Affairs management			Yes	
Regulatory & Register management	Yes			Yes
Cyber Security Training			Yes	
Resilience & Business Continuity Management	Yes	Yes	Yes	Yes
Finance and Resources management	Yes			
Reserves policy			Yes	
Estates	Yes	Yes	Yes	Yes
General Data Protection Act (GDPR)			Yes	Yes
Review of AGC activities & effectiveness, terms of reference				Yes
Legal Risks			Yes	
AGC Forward Plan	Yes	Yes	Yes	Yes
Session for Members and auditors	Yes	Yes	Yes	Yes
Other one-off items	Cabinet Office Counter Fraud Standards Whistle Blowing Policy Review			

Anti Fraud, Bribery and Corruption Policy

Strategic delivery:	☒ Setting standards	☒ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item			
Paper number	AGC (06/03/2019) 667 RS		
Meeting date	5 March 2019		
Author	Morounke Akingbola, Head of Finance		
Output:			
For information or decision?	For information		
Recommendation	The Committee is asked to agree the amended policy.		
Resource implications	None		
Implementation date	Ongoing		
Communication(s)	Ongoing		
Organisational risk	☒ Low	☐ Medium	☐ High
Annexes			
Annex A –	Counter Fraud and Anti-Theft Policy		

1. Purpose

1.1. The Counter Fraud and Anti- Theft Policy was implemented to ensure people working for the HFEA are aware that fraud can exist and how to respond if fraud is suspected.

1.2. This paper also confirms that a review of the HFEA Anti-Fraud Policy has been undertaken and to set out the updated policy which includes a few minor amendments for the committee's agreement.

2. Policy

2.1. The policy was shared with the Committee in 2015 and has since been reviewed and re-branded. The policy was shared with CMG in February who approved the updated policy, however the response plan was a late addition and will be shared post meeting.

2.2. The full final version will be shared with staff via the intranet and we are planning to have DHSC Anti-Fraud unit give a presentation to staff to supplement this policy.

2.3. Any comments or changes the Committee deems necessary are requested.

Human Fertilisation & Embryology Authority

Counter Fraud and Anti-Theft Policy

Introduction

1. This strategy has been produced in order to promote and support the framework within which the HFEA tackles fraud and theft and makes reference to the Bribery Act 2010. It sets out the aim and objectives of the Authority with respect to countering fraud and theft, whether it is committed externally or from within. Awareness of, and involvement in, counter-fraud and anti-theft work should be a general responsibility of all, and the support of all staff is needed. With clear direction from the CEO that there will be a zero-tolerance attitude to fraud within the HFEA.

.

Aim

2. It is the Authority's aim to generate an anti-fraud and theft culture that promotes honesty, openness, integrity and vigilance in order to minimise fraud and theft and its cost to the Authority.

Objectives

3. In respect of the risk of fraud and theft, the Authority seeks to:

- promote and support an anti-fraud and theft culture;
- deter, prevent and discover fraud and theft effectively;
- carry out prompt investigations of suspected fraud and theft;
- take effective action against individuals committing fraud and theft;
- support the core values and principles set out in the Civil Service Code

Protecting the Authority from the risk of fraud and theft

Promoting and supporting an anti-fraud and theft culture

4. The Authority seeks to foster an anti-fraud and theft culture in which all staff are aware of what fraud and theft are, and what actions constitute fraud and theft. Staff should know how to report suspicions of fraud and theft with the assurance that such suspicions will be appropriately investigated, and any information supplied will be kept in confidence.

5. This policy aims to promote good practice within the HTA through the following:

- zero tolerance to fraud;
- a culture in which bribery is never accepted;
- any allegations of fraud, anonymous or otherwise, will be investigated;
- consistent handling of cases without regard to position held or length of service
- consideration of whether there have been failures of supervision. Where this has occurred, disciplinary action may be initiated against those responsible;
- any losses resulting from fraud will be recovered, if necessary through civil actions
- publication of the anti-fraud policy on the HTA intranet site;
- all frauds will be reported to the Audit and Risk Assurance Committee.

Deterring, preventing and discovering fraud and theft

6. The preferred way of minimising fraud and theft is to deter individuals from trying to perpetrate a fraud or theft in the first place. An anti-fraud and anti - theft culture whereby such activity is understood as unacceptable, combined with effective controls to minimise the opportunity for fraud and theft, can serve as a powerful deterrent. The main deterrent is often the risk of being caught and the severity of the consequences. One of the most important aspects about deterrence is that it derives from perceived risk and not actual risk.

7. If it is not possible to deter individuals from committing frauds and thefts, then the next preferable course of action is to prevent them from succeeding before there is any loss. Potential/possible frauds and thefts will be identified and investigated through:

   - a defined counter-fraud and anti-theft assurance programme addressing the areas where the Authority is most vulnerable to fraud and theft. Any gaps in control or areas where controls are not being applied properly that are identified by this work will be addressed accordingly; and

   - routine use of Computer Assisted Audit Techniques (CAATs) as a standard part of the internal auditor's toolkit, to identify transactions warranting further investigation.

8. It is the responsibility of managers to ensure that there are adequate and effective controls in place. Internal Audit will provide assurance on the adequacy and effectiveness of such controls. In addition to the annual programme of internal audits (which provide assurance on the controls identified in the Strategic Risk Register), Internal Audit will also carry out advisory work on request and seek to ensure appropriate controls are built into new systems and processes through its project assurance role.

9. It will not always be possible to prevent frauds and thefts from occurring. Therefore, the Authority must have the means to discover frauds and thefts at the earliest opportunity. All staff should be vigilant and aware of the potential for fraud and theft and report any suspicions in accordance with the Authority's Whistleblowing Policy

Prompt investigation of suspected frauds and thefts

10. All suspected and actual frauds will be investigated promptly in line with the Whistleblowing Policy. The effective investigation of suspected and actual frauds depends upon the capability of the appropriate staff or internal auditors conducting these investigations.

11. All thefts should be reported to the relevant line manager for action to be taken in line with the Authorities policies.

Taking effective action

12. In the case of a proven allegation of fraud or theft, effective action will be taken in respect of those investigated in accordance with the Authority's Disciplinary Policies and Procedures. The Authority will always seek financial redress in cases of losses to fraud and theft and legal action will be taken where appropriate.

Policy Statement

13. The HFEA requires all staff at all times to act honestly and with integrity and to safeguard the public resources for which they are responsible. The Authority will not accept any level of fraud, corruption or theft. Consequently, any suspicion or allegation of fraud or theft will be investigated thoroughly and dealt with appropriately. The Authority is committed to ensuring that opportunities for fraud, corruption or theft are reduced to the lowest possible level.

14. Staff should have regard to related policy and procedures including:

    a. HFEA Standing Financial Instructions and Financial Procedures
    b. HFEA Staff Handbook
    c. Disciplinary and Whistleblowing Policies

15. This Policy applies to all staff including contractors, temporary staff and third parties delivering services to and on behalf of the Authority.

16. The circumstances of individual frauds and thefts will vary. The Authority takes fraud and theft very seriously. All cases of actual or suspected fraud or theft against the Authority will be thoroughly and promptly investigated and appropriate action will be taken.

Definitions of Fraud and Theft, Bribery and Corruption

17. The Fraud Act 2006 created the general offence of fraud which can be committed in three ways. These are by false representation, by failing to disclose information where there is a legal duty to do so, and by abuse of position. It also created offences of obtaining services dishonestly and of possessing, making and supplying articles for use in frauds.

18. A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it.

19. A bribe is an inducement or reward offered, promised or provided in order to gain any commercial, contractual, regulatory or personal advantage. The advantage sought or the inducement offered does not have to be financial or remunerative in nature, and may take the form of improper performance of an activity or function.

20. The Bribery Act 2010 includes the offences of:

    a) Section 1 – bribing another person;
    b) Section 2 – offences relating to being bribed.

21. Further guidance is at http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf

22. Corruption is defined as “The offering, giving, soliciting or acceptance of an inducement or reward which may influence the action of any person”. In addition “the failure to disclose an interest in order to gain financial or other pecuniary gain”.

23. The HFEA’s responsibilities in relation to fraud are set out in Annex 4.9 of Managing Public Money https://www.gov.uk/government/publications/managing-public-money

Avenues for reporting Fraud and Theft

24. The Authority has a Whistleblowing Policy that sets out how staff should report suspicions of fraud, including the process for reporting thefts. All frauds, thefts, or suspicions of fraud or theft, of whatever type, should be reported in accordance with the Whistleblowing Policy. All matters will be dealt with in confidence and in strict accordance with the terms of the Public Interest Disclosure Act 1998. This statute protects the legitimate personal interests of staff.

Responsibilities

25. The responsibilities of Authority staff in respect of fraud and theft are determined by the Treasury publication “Managing Public Money” (MPM), supplemented by the Authority’s policies and procedures for financial and corporate governance. These documents include Standing Financial Instructions, Financial Procedures; Standing Orders, the Financial Memorandum, and the Management Statement

Accounting Officer (Chief Executive)

26. As “Accounting Officer”, the Chief Executive is responsible for managing the organisation’s risks, including the risks of fraud and theft, from both internal and external sources. The risks of fraud or theft are usually measured by the probability of them occurring and their impact in monetary and reputational terms should they occur. In broad terms, managing the risks of fraud and theft involves:

    a. assessing the organisation’s overall vulnerability to fraud and theft;
    b. identifying the areas most vulnerable to fraud and theft;
    c. evaluating the scale of fraud and theft risk;

d. responding to the fraud and theft risk;
e. measuring the effectiveness of managing the risk of fraud and theft;
f. reporting fraud and theft to the Treasury;
g. In consultation with the Chair, Director of Finance and Resources, and Legal Services, reporting any thefts against the Authority to the police.

27. In addition, the Chief Executive must:

a. be satisfied that the internal control applied by the Authority conforms to the requirements of regularity, propriety and good financial management;
b. ensure that adequate internal management and financial controls are maintained by the Authority, including effective measures against fraud and theft.

28. The Chief Executive will be responsible for making a decision as to whether:

a. an individual who is under suspicion of fraud or theft should be suspended;
b. criminal or disciplinary action should be taken against an individual who is found to have committed a fraud or theft.

29. Such decisions should be taken in conjunction with the relevant Director, HR Manager and Internal Audit, with advice from Legal Services and Finance where appropriate, to ensure consistency across the organisation. Should there be any disagreement over the appropriate action to be taken, the Chief Executive will be the final arbiter in deciding whether criminal or disciplinary action should be taken against an individual.

Director of Finance and Resources

30. Responsibility for overseeing the management of fraud and theft risk within the Authority has been delegated to the Director of Finance and Resources, whose responsibilities include:

b. ensuring that the Authority's use of resources is properly authorised and controlled;
c. developing fraud and theft risk profiles and undertaking regular reviews of the fraud and theft risks associated with each of the key organisational objectives in order to ensure the Authority can identify, itemise and assess how it might be vulnerable to fraud and theft;
d. evaluating the possible impact and likelihood of the specific fraud and theft risks the Authority has identified and, from this, deducing a priority order for managing the Authority's fraud and theft risks;
e. designing an effective control environment to prevent fraud and theft commensurate with the fraud and theft risk profiles. This will be underpinned by a balance of preventive and detective controls to tackle and deter fraud, corruption and theft;
f. ensuring that appropriate reporting of fraud and theft takes place both within the organisation and to the Audit and Governance Committee, and to the Assurance Control and Risk (ACR) team within H M Treasury, to which any novel or unusual frauds must be reported, as well as preparing the required annual fraud return of the Authority to H M Treasury which also includes a requirement to report actual or attempted thefts;

g. forward to the Department of Health and Social Care an annual report on fraud and theft suffered by the Authority; notify any unusual or major incidents as soon as possible; and notify any changes to internal audit's terms of appointment, the Audit and Governance Committee's terms of reference or the Authority's Fraud and Anti – Theft Policy.

h. measuring the effectiveness of actions taken to reduce the risk of fraud and theft. Assurances about these measures will be obtained from Internal Audit, stewardship reporting, control risk self-assessment and monitoring of relevant targets set for the Authority;

i. establishing the Authority's response to fraud and theft risks including mechanisms for:

    - developing a counter-fraud and anti-theft policy, a fraud response plan and a theft response plan;
    - developing and promoting a counter-fraud and anti-theft culture;
    - allocating responsibilities for the overall management of fraud and theft risks and for the management of specific fraud and theft risks so that these processes are integrated into management generally;
    - establishing cost-effective internal controls to detect and deter fraud and theft, commensurate with the identified risks;
    - developing skills and expertise to manage fraud and theft risk effectively and to respond to fraud and theft effectively when it arises;
    - establishing well publicised avenues for staff and members of the public to report their suspicions of fraud and theft;
    - responding quickly and effectively to fraud and theft when it arises using trained and experienced personnel to investigate where appropriate;
    - establishing systems to monitor the progress of investigations;
    - using Internal Audit to track all fraud cases and drawing on their experience to strengthen control to reduce the risk of recurrence of frauds and thefts;
    - reporting thefts to the policy in accordance with the theft response plan;
    - seeking to recover losses;
    - continuously evaluating the effectiveness of counter-fraud and anti-theft measures in reducing fraud and theft respectively;
    - working with stakeholders to tackle fraud and theft through intelligence sharing, joint investigations and so on.

j. as Director of Finance and Resources, enforcing financial compliance across the organisation while guarding against fraud and theft and delivering continuous improvement in financial control.

k. In consultation with the Chief Executive, Chair and legal services, reporting any thefts against the Authority to the police.

31. Managers are responsible for:

a. ensuring that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively, in order to assist in their role of preventing and detecting fraud and theft;

b. assessing the types of risk involved in the operations for which they are responsible;

c. reviewing and testing the control systems for which they are responsible regularly;

d. ensuring that controls are being complied with and their systems continue to operate effectively;

e. implementing new controls to reduce the risk of similar frauds and thefts taking place;

f. ensuring that all expenditure is legal and proper;

g. authorising losses of cash including theft and fraud in accordance with Financial Delegation limits;

h. reporting any fraud, or suspicion of fraud in accordance with the Whistleblowing Policy;

Staff

32. All staff, individually and collectively, are responsible for avoiding loss and for:

a. acting with propriety in the use of official resources and the handling and use of public funds whether they are involved with cash or payments systems, receipts or dealing with suppliers;

b. conducting themselves in accordance with the seven principles of public life set out in the first report of the Nolan Committee "Standards in Public Life". These are:

- Selflessness: Holders of public office should take decisions solely in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family, or their friends;
- Integrity: Holders of public office should not place themselves under any financial or other obligation to outside individuals or organisations that might influence them in the performance of their official duties;
- Objectivity: In carrying out public business, including making public appointments or recommending individuals for rewards and benefits, holders of public office should make choices on merit;
- Accountability: Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office;
- Openness: Holders of public office should be as open as possible about all the decisions and action that they take. They should give reasons for their decisions and restrict information only when the wider public interest clearly demands it;
- Honesty: Holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interest (CCE 4);
- Leadership: Holders of public office should promote and support these principles by leadership and example.

c. being alert to the possibility that unusual events or transactions could be indicators of fraud or theft;

d. reporting details immediately through the appropriate channel if they suspect that a fraud or theft has been committed or see any suspicious acts or events;

e. co-operating fully with whoever is conducting internal checks or reviews, or investigations of fraud or theft.

33. Staff are specifically not responsible for investigating any allegations of fraud or theft. These are to be undertaken in accordance with the Authority's Public Interest Disclosure ("Whistleblowing" Policy).

Board Members

34. The Authority's Board Members have a responsibility to:

a. comply at all times with the Code of Practice that is adopted by the Authority and with the rules relating to the use of public funds and to conflicts of interest, and declare any interests which are relevant and material to the board:

b. not misuse information gained in the course of their public service for personal gain or for political profit, nor seek to use the opportunity of public service to promote their private interests or those of connected persons or organisations:

c. comply with the Authority's rules on the acceptance of gifts and hospitality and of business appointments.

Internal Audit

35. Matters in relation to fraud and/or corruption will involve the Authority's Internal Auditors.

Internal Audit's primary responsibilities in relation to fraud are:

a. delivering an opinion to the Chief Executive on the adequacy of arrangements for managing the risk of fraud and ensuring that the Authority promotes an anti-fraud culture;

b. assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of control commensurate with the extent of the potential exposure/risk in the various segments of the Authority's operations;

c. ensuring that management has reviewed its risk exposures and identified the possibility of fraud as a risk;

d. assisting management by conducting fraud investigations;

36. Under its approved terms of appointment, the Internal Auditors may be tasked with responsibility for investigating cases of discovered fraud and corruption within, or operated against, the Authority.

Audit and Governance Committee

37. The Audit and Governance Committee is responsible for:

a. Receiving reports on losses and compensations, and overseeing action in response to these;

b. Ensuring that the Authority has in place an appropriate fraud policy and fraud response plan.

Review

38. This policy will be reviewed every two years or when there are changes in the law that significantly affect this policy.

References

Managing Public Money – Chapter 4 and Annex 4.7 (HM Treasury);

Managing the Risk of Fraud (HM Treasury) : www.hm-treasury.gov.uk

Core Values and the Civil Service Code : www.civilservice.gov.uk/about/values/index.aspx

Related Authority Corporate Documents

Financial Memorandum

Management Statement

Standing Financial Instructions

Standing Orders

Disciplinary Policy & Procedure

Whistleblowing Policy

Staff Handbook Audit and Governance Committee Terms of Reference

Document name	Counter Fraud and Anti-Theft Policy
Release date	March 2019
Author	Head of HR
Approved by	CMG
Next review date	March 2021
Total pages	14

Version/revision control

Version	Changes	Updated by	Approved by	Release date
2.0	Revisions/update	Head of Finance	CMG	May 2012
2.1	Revision/updates	Head of Finance	AGC	March 2015
2.2	Minor clarification under staff para	Head of Finance		
2.3	Reviewed/re-branded	Head of Finance	CMG	March 2019

APPENDIX

(Suggested) Fraud response plan

Introduction

1. The fraud response plan provides a checklist of actions and a guide to follow in the event that fraud is suspected. Its purpose is to define authority levels, responsibilities for action and reporting lines in the event of suspected fraud, theft or other irregularity. It covers:

   a) notifying suspected fraud;
   b) the investigation process;
   c) liaison with police and external audit;
   d) initiation of recovery action;
   e) reporting process;
   f) communication with the Audit and Risk Assurance Committee.

Notifying suspected fraud

2. It is important that all staff are able to report their concerns without fear of reprisal or victimisation and are aware of the means to do so. The Public Interest Disclosure Act 1998 (the "Whistleblowers Act") provides appropriate protection for those who voice genuine and legitimate concerns through the proper channels.

3. In the first instance, any suspicion of fraud, theft or other irregularity should be reported, as a matter of urgency, to your line manager. If such action would be inappropriate, your concerns should be reported upwards to one of the following:

   a) your Head;
   b) your Director;
   c) Chief Executive;
   d) Audit and Governance Committee Chair;

4. Additionally, all concerns must be reported to the Director of Finance and Resources.

5. Every effort will be made to protect an informant's anonymity if requested. However, the HFEA will always encourage individuals to be identified to add more validity to the accusations and allow further investigations to be more effective. In certain circumstances, anonymity cannot be maintained. This will be advised to the informant prior to release of information.

6. If fraud is suspected of the Chief Executive or Director of Finance and Resources, notification must be made to the Audit and Governance Committee Chair who will use suitable discretion and coordinate all activities in accordance with this response plan, appointing an investigator to act on their behalf.

7. If fraud by an Authority Member is suspected, it should be reported to the Chief Executive and the Director of Finance and Resources who must report it to the Chair to investigate. If fraud by the Chair

is suspected, it should be reported to the Chief Executive and Director of Finance and Resources who must report it to the Chair of the Audit and Governance Committee to investigate.

The investigation process

8. Suspected fraud must be investigated in an independent, open-minded and professional manner with the aim of protecting the interests of both the HFEA and the suspected individual(s). Suspicion must not be seen as guilt to be proven.

9. The investigation process will vary according to the circumstances of each case and will be determined by the Chief Executive in consultation with the Director of Finance and Resources. The process is likely to involve the DHSC Anti-Fraud Unit, who have expertise and resources to undertake investigations. An "Investigating Officer" will be appointed to take charge of the investigation on a day-to-day basis.

10. The Investigating Officer will appoint an investigating team. This may, if appropriate, comprise staff from within the Finance Directorate but may be supplemented by others from within the HFEA or from outside.

11. Where initial investigations reveal that there are reasonable grounds for suspicion, and to facilitate the ongoing investigation, it may be appropriate to suspend an employee against whom an accusation has been made. This decision will be taken by the Chief Executive in consultation with the Director of Finance and Resources, the Head of HR and the Investigating Officer. Suspension should not be regarded as disciplinary action nor should it imply guilt. The process will follow the guidelines set out in HFEA Disciplinary policy relating to such action.

12. It is important, from the outset, to ensure that evidence is not contaminated, lost or destroyed. The investigating team will therefore take immediate steps to secure physical assets, including computers and any records thereon, and all other potentially evidential documents. They will also ensure, in consultation with the Director of Finance and Resources, that appropriate controls are introduced in prevent further loss.

13. The Investigating Officer will ensure that a detailed record of the investigation is maintained. This should include chronological files recording details of all telephone conversations, discussions, meetings and interviews (with whom, who else was present and who said what), details of documents reviewed, tests and analyses undertaken, the results and their significance. Everything should be recorded, irrespective of the apparent insignificance at the time.

14. All interviews will be concluded in a fair and proper manner and as rapidly as possible.

15. The findings of the investigation will be reported to the Chief Executive and Director of Finance and Resources. Having considered, with the Head of HR, the evidence obtained by the Investigating officer, the Chief Executive and Director of Finance and Resources will determine what further action (if any) should be taken**.**

Liaison with police & external audit

16. Some frauds will lend themselves to automatic reporting to the police (such as theft by a third party). For other frauds the Chief Executive, following consultation with the Director of Finance and Resources and the Investigating Officer will decide if and when to contact the police.

17. The Director of Finance and Resources will report suspected frauds to the police and external auditors at an appropriate time.

18. All staff will co-operate fully with any police or external audit enquiries, which may have to take precedence over any internal investigation or disciplinary process. However, wherever possible, teams will co-ordinate their enquiries to maximize the effective and efficient use of resources and information.

Initiation of recovery action

19. The HFEA will take appropriate steps, including legal action if necessary, to recover any losses arising from fraud, theft or misconduct. This may include action against third parties involved in the fraud or whose negligent actions contributed to the fraud.

Reporting process

20. Throughout any investigation, the Investigating Officer will keep the Chief Executive and the Director of Finance and Resources informed of progress and any developments. These reports may be oral or in writing.

21. On completion of the investigation, the Investigating Officer will prepare a full written report to the Chief Executive and Director of Finance and Resources setting out:

    a) background as to how the investigation arose;
    b) what action was taken in response to the allegations;
    c) the conduct of the investigation;
    d) the facts that came to light and the evidence in support;
    e) recommended action to take against any party where the allegations were proved (see policy on disciplinary action where staff are involved);
    f) recommended action to take to recover any losses;
    g) recommendations and / or action taken by management to reduce further exposure and to minimise any recurrence.

22. In order to provide a deterrent to other staff a brief and anonymous summary of the circumstances will be communicated to staff.

Communication with the Audit and Governance Committee

23. Irrespective of the amount involved, all cases of attempted, suspected or proven fraud must be reported to the Audit and Governance Committee by the Chief Executive or Director of Finance and Resources.

24. The Audit and Governance Committee will notify the Authority.

25. In addition, the Department requires returns of all losses arising from fraud together with details of:

    a) all cases of fraud perpetrated within the HFEA by members of its own staff, including cases where staff acted in collusion with outside parties;
    b) all computer frauds against the HFEA, whether perpetrated by staff or outside parties;
    c) all cases of suspected or proven fraud by contractors arising in connection with contracts placed by the HFEA for the supply of goods and services.

26. The Director of Finance and Resources is responsible for preparation and submission of fraud reports to the Audit and Risk Assurance Committee and the Department.

Public Interest Disclosure ("Whistleblowing") Policy

Strategic delivery:	☒ Setting standards	☒ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item			
Paper number	AGC (06/03/2019) 668 MA		
Meeting date	06 March 2019		
Author	Yvonne Akinmodun, Head of Human Resources		
Output:			
For information or decision?	For information		
Recommendation	The Committee is asked to agree the amended policy.		
Resource implications	None		
Implementation date	Ongoing		
Communication(s)	Ongoing		
Organisational risk	☒ Low	☐ Medium	☐ High
Annexes			
Annex A –	Whistleblowing Policy		

1. Purpose

1.1. The Public Interest Disclosure Policy generally referred to as the “Whistleblowing” Policy was implemented to ensure people working for the HFEA were aware of the channels available to report inappropriate behaviour.

1.2. This paper also confirms that a review of the HFEA Whistleblowing Policy has been undertaken and to set out the updated policy which includes a few minor amendments for the committee’s agreement.

2. Policy

2.1. The policy was shared with the Staff Forum and tabled at CMG who approved the draft policy. In December 2014, a number of minor amendments were proposed by CMG. The Committee approved the policy in December 2016.

2.2. A review was not undertaken in 2017 due to staff and work commitments and therefore was not presented to AGC for approval.

2.3. We have now reviewed the policy and have updated names where appropriate.

2.4. Any comments or changes the Committee deems necessary are requested.

Human Fertilisation & Embryology Authority

Public Interest Disclosure ("Whistleblowing") Policy

1. Introduction

1.1 In accordance with the Public Interest Disclosure Act 1998, and the corporate values of integrity, impartiality, fairness and best practice, this policy intends to give employees a clear and fair procedure to make disclosures which they feel are in the public interest ("whistleblowing") and will enable the HFEA to investigate these disclosures promptly and correctly.

2. Aim

2.1 To outline what constitutes a Public Interest disclosure, and to provide a procedure within the HFEA to deal with such disclosures

3. Scope

3.1 This policy applies to all employees, both permanent and fixed term and also Authority members

4. Responsibility

4.1 The HR department is responsible for ensuring that all staff have access to this policy. Managers and Senior Executives are responsible for ensuring that any public interest disclosure is dealt with immediately, and sensitively, and confidentially.

5. Principles

5.1 Employees who raise their concerns within the HFEA, or in certain circumstances, to prescribed external individuals or bodies will not suffer detriment as a result of their disclosure, this includes protection from subsequent unfair dismissal, victimisation or any other discriminatory action.

5.2 The Public Interest Disclosure Act 1998, (more widely known as the 'Whistleblowers' Act) protects 'workers' from suffering any detriment where they make a disclosure of information while holding a reasonable belief that the disclosure tends to show that:

(a) a criminal offence has been committed, is being committed or is likely to be committed,
(b) a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject,
(c) A miscarriage of justice has occurred, is occurring or is likely to occur,
(d) The health and safety of any individual has been, is being or is likely to be endangered,
(e) The environment has been, is being or is likely to be damaged, or
(f) Information tending to show any matter falling within any one of the preceding paragraphs has been, is being or is likely to be deliberately concealed.

5.3 It should be noted that disclosures which in themselves constitute an offence are <u>not</u> protected.

5.4 HFEA's policy is intended to ensure that where a member of staff, including temporary or contractual staff, have concerns about criminal activity and/or serious malpractice e.g. fraud, theft, or breaches of policy on health and safety, they can be properly raised and resolved in the workplace. Such matters **must be raised internally** in the first instance. Please refer to the paragraph on gross misconduct in the Authority's Disciplinary Policy, and also the Authority's counter-fraud and anti-theft policy.

5.5 HFEA seeks to foster a culture that enables staff who witness such malpractice to feel confident to raise the matter in the first instance in the knowledge that, once raised, it will be dealt with effectively and efficiently. The HFEA will not tolerate the victimisation of individuals who seek to bring attention to matters of potentially serious public concern, and will seek to reassure any individual raising a concern that he or she will not suffer any detriment for doing so. If an individual is subject to a detriment for raising a concern the HFEA will seek to pursue an appropriate sanction.

5.6 Frivolous or vexatious claims which fall outside the protection of the Act or such other provisions as may be held to protect them (e.g. HFEA's codes of conduct, confidentiality clause etc.) may be considered acts of misconduct and subject to disciplinary action.

6. Procedure

Internal Disclosure

6.1 HFEA staff who become concerned about the legitimacy or public interest aspect of any HFEA activity or management of it should raise the matter initially with their line manager. If a member of staff feels unable to raise the matter through their line manager, they may do so through the HR Department.

6.2 It will be the responsibility of the line manager to record and pursue the concerns expressed; consulting such other parts of the Authority; (e.g. HR, SMT) as may be necessary, including where appropriate consideration as to whether external expert assistance is required.

6.3 The identity of the individual making the disclosure will be kept confidential if the staff member so requests unless disclosure is required by law.

6.4 In other than serious cases, the line manager will normally be responsible for responding to the individual's concern. They must maintain appropriate records and ensure that they provide the individual raising the concern with:

- An explanation of how and by whom the concern will be handled
- An estimate of how long the investigation will take
- Where appropriate, the outcome of the investigation
- Details of who he/she should report to if the individual believes that he/she is suffering a detriment for having raised the concern
- Confirmation that the individual is entitled to independent advice.

6.5 Should a member of staff feel that they are not satisfied that their concern has been adequately resolved, they may raise the matter more formally with the Chief Executive.

6.6 Any member of staff wishing to make a disclosure of significant importance may approach the Chief Executive in the first instance. Matters of significant importance include, but are not restricted to, criminal activity e.g. fraud or theft, or other breaches of the law; miscarriage of justice; danger to health and safety; damage to the environment; behaviour or conduct likely to undermine the Authority's functions or reputation; breaches of the *Seven Principles of Public Life* (Annex A) and attempts to cover up such malpractice.

6.7 The matter of significant importance may have taken place in the past, the present, or be likely to take place in the future.

6.8 Concerns may be raised either in writing or at a meeting convened for the purpose. A written record of meetings must be made and agreed by those present. In serious cases or in any case where a formal investigation may be required, line managers concerned should consult the Head of HR and SMT, unless they are implicated, when they should speak to the Chair. Line managers must not take any action which might prejudice any formal investigation, or which might alert any individual to the need to conceal or destroy any material evidence.

6.9 Where an individual has reason to believe that the concerns about which he / she intends to make a disclosure are condoned or are being concealed by the line manager to whom they would ordinarily be reported, the matter may be referred directly to the Head of HR who will determine in conjunction with the Chief Executive the need for, and the means of, investigation. In exceptional circumstances, the Head of HR may take the disclosure directly to the HFEA Chair. Any such approach should be made in writing, clearly stating the nature of the allegations.

6.10 Unless inappropriate in all the circumstances, investigations will normally be undertaken by the following posts:

Allegation against	*Investigated by*
Directors	Chief Executive
Chief Executive	Chair
Members	Chair
Audit Committee Member	Audit Committee Chair
Chair	Department of Health*
Deputy Chair	Chair

*Via Senior Sponsor at the DHSC (currently Mark Davies, Director, Health Science and Bioethics (tel. 0207 210 6304 / mark.davies@dh.gsi.gov.uk)

6.11 Individuals under contract to the HFEA for the delivery of services should raise any issues of concern in the same way, via the appropriate line manager.

6.12 Once investigations and follow up actions as appropriate have been concluded, a written summary of the matter(s) reported and concluding actions taken should be forwarded to the Chair of the Authority (the Chair) for inclusion in the central record of issues reported under this policy. The anonymity of the individual who made the disclosure should be preserved as far as possible.

External Disclosure

6.13 The HFEA recognises that there are circumstances where the matters raised cannot be dealt with internally and in which an individual may make the disclosure externally and retain the employment protection of the Act. Ordinarily such disclosure will have to be to a person or regulatory body prescribed by an order made to the Secretary of State for these purposes.

6.14 Prescribed bodies under the Act include the Comptroller and Auditor General of the National Audit Office (NAO), who are the external auditors to the Authority. The Act states that disclosure to the NAO should relate to "the proper conduct of public business, fraud, value for money and corruption in relation to the provision of centrally-funded public services."

6.15 The NAO have a designated whistle blowing hotline which can be used in confidence on 020 7798 7999. Further information about this service and other bodies prescribed under the Act is available via the NAO's website: http://www.nao.org.uk/contact-us/whistleblowing-disclosures/

6.16 In these circumstances the worker will be obliged to show that the disclosure is made in good faith and not for personal gain, that he or she believed that the information provided and allegation made were substantially true, and that they reasonably believed that the matter fell within the description of matters for which the person or regulatory body was prescribed.

6.17 Unless the relevant failure of the employer is of an exceptionally serious nature, the worker **will not** be entitled to raise it publicly unless he/she has already raised it internally, and/or with a prescribed regulatory body and, in all the circumstances, it is reasonable for him / her to make the disclosure in public.

6.18 If a member of staff is unsure of their rights or obligations and wishes to seek alternative independent advice**,** Public Concern at Work is an independent organisation that provides confidential advice, free of charge, to people concerned about wrongdoing at work but who are not sure whether or how to raise the concern (telephone 020 7404 6609 or 020 3117 2520, email: whistle@pcaw.org.uk), or visit their website at http://www.pcaw.org.uk/. HFEA staff may also use the **Whistleblowing Helpline**, which offers free, confidential and anonymous advice to the health sector: http://wbhelpline.org.uk/

6.19 Where matters raised from external disclosure procedures are (as appropriate) subsequently investigated and resolved internally, a written record of the matters raised and actions taken should be forwarded to the Chair for inclusion in the central record of issues referred under this policy. The anonymity of the individual who made the disclosure should be preserved as far as possible.

Information held on the HFEA Register

Under Section 31 of the Human Fertilisation and Embryology Act 1990 ("the Act"), the HFEA is required to keep a register containing certain categories of information. The Act prohibits disclosure of data held on the HFEA register, subject to a number of specified exceptions. Disclosure of information which is not permitted by an exception may constitute a criminal offence.

7. Notes

7.1 This policy will be reviewed by the Audit and Governance Committee annually.

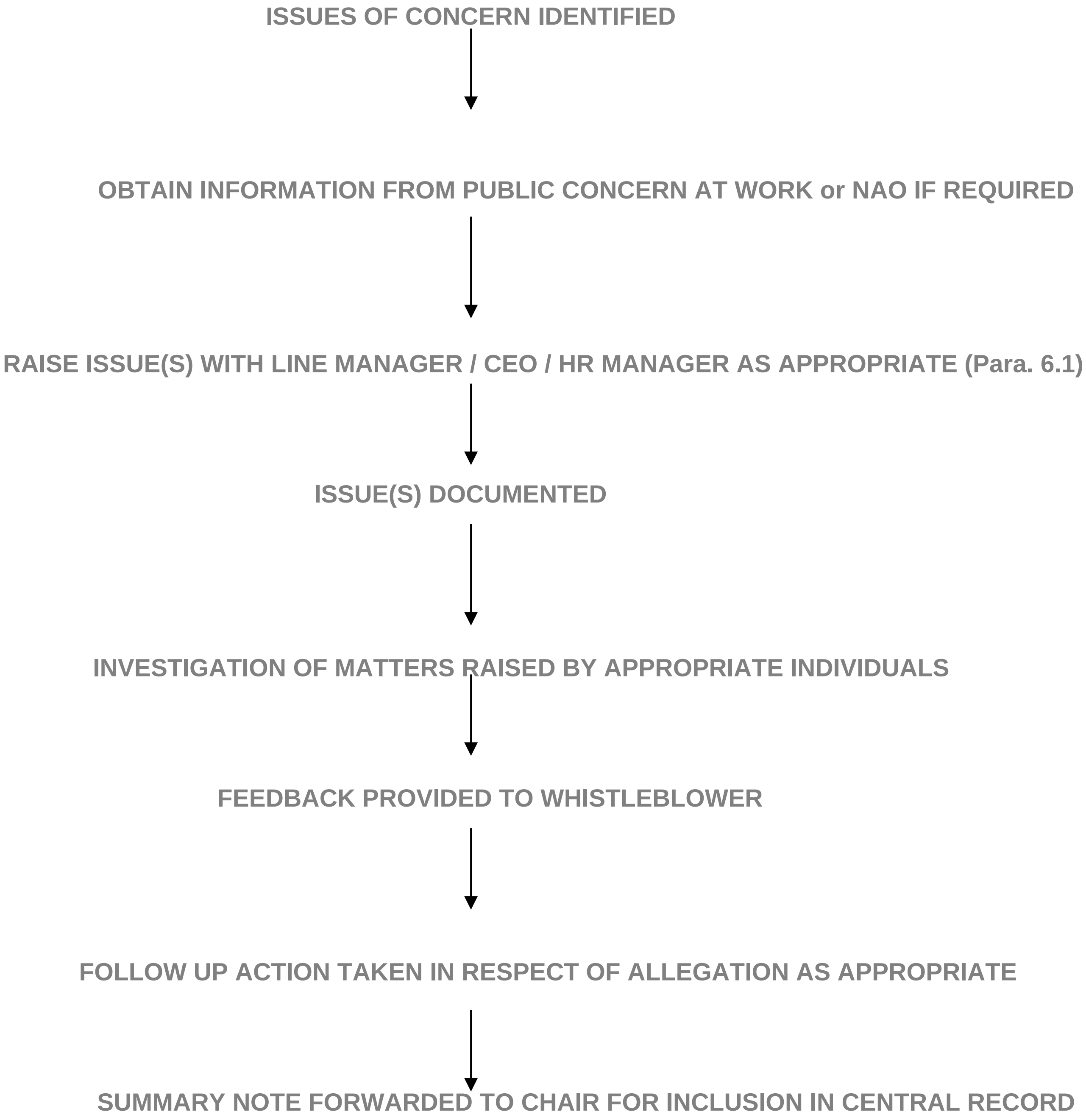
7.2 An anonymised summary of issues raised under this whistleblowing policy and remedial actions taken will be forwarded annually to the Authority for information.

7.3 The role of the HFEA as a regulatory body:

Under the provisions of the Public Interest Disclosure Act 1998 employees of an organisation are able to disclose publicly (under certain circumstances) their concerns about legitimacy or public interest aspects of the organisation within which they work. Although the Act requires that concerns be raised internally in the first instance, there are provisions for disclosure to be made to a regulatory body. The HFEA is itself one such regulatory body.

The procedure for dealing with a public interest disclosure from a member of staff of one of the licensed centres for which the HFEA is the regulatory body is not covered by this policy and prior to any separate procedure being issued, guidance must be sought from the Director of Compliance and Information.

Procedure Diagram



ISSUES OF CONCERN IDENTIFIED

OBTAIN INFORMATION FROM PUBLIC CONCERN AT WORK or NAO IF REQUIRED

RAISE ISSUE(S) WITH LINE MANAGER / CEO / HR MANAGER AS APPROPRIATE (Para. 6.1)

ISSUE(S) DOCUMENTED

INVESTIGATION OF MATTERS RAISED BY APPROPRIATE INDIVIDUALS

FEEDBACK PROVIDED TO WHISTLEBLOWER

FOLLOW UP ACTION TAKEN IN RESPECT OF ALLEGATION AS APPROPRIATE

SUMMARY NOTE FORWARDED TO CHAIR FOR INCLUSION IN CENTRAL RECORD

Procedures for **external disclosures** will depend upon the procedures of the body to whom disclosures are made. **Public Concern at Work** or the **NAO** will be able to provide information in this respect. Where matters raised from external disclosure procedures are (as appropriate) subsequently investigated and resolved internally, a written record of the matters raised and actions taken should be forwarded to the Chair for inclusion in the central record of issues referred under this policy.

The identity of the individual making the disclosure will be kept confidential if the staff member so requests unless disclosure is required by law.

Seven Principles of Public Life
(As recommended by the Committee on Standards in Public Life)

Selflessness

Holders of public office should take decisions solely in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family or their friends.

Integrity

Holders of public office should not place themselves under any financial or other obligation to outside individuals or organisations which might influence them in the performance of their official duties.

Objectivity

In carrying out public business, including making public appointments, awarding contracts, or recommending individuals for rewards or benefits, holders of public office should make choices on merit.

Accountability

Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office.

Openness

Holders of public office should be as open as possible about all decisions and actions that they take. They should give reasons for their decisions and restrict information only when the wider public interest clearly demands.

Honesty

Holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interests.

Leadership

Holders of public office should promote and support these principles by leadership and example.

These principles apply to all aspects of public life.

Document name	Public Interests Disclosure
Doc Ref No.	2014/021228
Release date	10 December 2014
Author	Head of HR
Approved by	CMG/AGC/Staff Forum
Next review date	December 2018
Total pages	9

Version/revision control

Version	Changes	Updated by	Approved by	Release date
0.1	Created	Head of Finance	Head of HR	July 2010
0.2	Revisions and updates	Head of Finance	CMG/AGC/ Staff Forum	May 2012
0.3	Revisions and updated	Head of HR	Staff Forum/CMG/ AGC	December 2014
0.4	Minor clarification in 6.8 omitted at time of (0.3 above)	Head of HR	As above	February 2015
0.5	Reviewed/updated prior to AGC	Head of Finance and Head of HR		*December 2016*
0.6	Reviewed/updated prior to AGC	Head of Finance and Head of HR		March 2019