Audit and Governance Committee meeting - agenda

22 June 2021

Online

Agenda item		Page No	Time
1.	Welcome, apologies and declaration of interests		10.00am
2.	Minutes of 16 March 2021 [AGC (22/06/2021) DO]	for decision	10.05am
3.	Matters arising [AGC (22/06/2021) MA]	for information	10.10am
4.	Digital programme update [AGC (22/06/2021) KH]	for information	10.20am
5.	Internal audit progress report [AGC (22/06/2021) JC]	for information	10.50am
6.	Implementation of recommendations [AGC (22/06/2021) MA]	for information	11.05am
7.	Information assurance and security (SIRO report) [AGC (22/06/2021) RS]	for information	11.15am
8.	Annual report and accounts (incl. annual governance statement) [AGC (22/06/2021) RS]	for decision	11.30am
9.	External audit completion report [AGC (22/06/2021) MS]	for information	11.50am 12.05pm
10.	Strategic risk register [AGC (22/06/2021) HC]	for comment	12.05pm
11.	Bi-annual human resource report [AGC (22/06/2021) YA]	for comment	12.20pm
12.	Resilience & business continuity management [AGC (22/06/2021) DH]	for comment	12.35pm
13.	AGC forward plan [AGC (22/06/2021) MA]	for decision	12.50pm
14.	Items for noting • Gifts and hospitality	for information	12.55pm

- Whistle blowing and fraud
- Contracts and Procurement

[AGC (22/06/2021) RS]

15.	Any other business	1.00pm
16.	Close	1.05pm
17.	Session for members and auditors only	

Next Meeting: Tuesday, 5 October 2021, Online

Minutes of Audit and Governance Committee meeting 16 March 2021

Details:			
Area(s) of strategy this paper relates to:	The best care – effective and ethical care for everyone The right information – to ensure that people can access the right information at the right time Shaping the future – to embrace and engage with changes in the law, science and society		
Agenda item	2		
Meeting date	22 June 2021		
Author	Debbie Okutubo, Governance Manager		
Output:			
For information or decision?	For decision		
Recommendation	Members are asked to confirm the minutes of the Audit and Governance Committee meeting held on 16 March 2021 as a true record of the meeting		
Resource implications			
Implementation date			
Communication(s)			
Organisational risk	☒ Low	☐ Medium	☐ High
Annexes			

Minutes of the Audit and Governance Committee meeting on 16 March 2021 held via teleconference

Members present	Anita Bharucha - Chair Margaret Gilmore Catharine Seddon Mark McLaughlin Geoffrey Podger
Apologies	None
External advisers	Mike Surman, National Audit Office – External auditor Joanne Charlton, Internal Auditor – GIAA
Observer	Csenge Gal, Department of Health and Social Care - DHSC
Staff in attendance	Peter Thompson, Chief Executive Richard Sydee, Director of Finance and Resources Clare Ettinghausen, Director of Strategy and Corporate Affairs Rachel Cutting, Director of Compliance and Information Morounke Akingbola, Head of Finance Dan Howard, Chief Information Officer Helen Crutcher, Risk and Business Planning Manager Debbie Okutubo, Governance Manager

1. Welcome, apologies and declarations of interest

1.1. The Chair welcomed everyone present online, in particular, Catharine Seddon as this was her first AGC meeting. Continuing, the Chair commented that Catharine became a member of the Authority in January, attended the PRISM Oversight meeting earlier in the month, and would take over as Chair of AGC later on in the year.

1.2. Catharine gave a brief overview of her career to date.

1.3. There were no apologies from Members.

1.4. There were no declarations of interest.

2. Minutes of the meeting held 8 December 2020

2.1. The minutes of the meeting held on 8 December were agreed as a true record and signed by the Chair.

3. Matters arising

3.1. The Head of Finance gave an update on matters arising. It was noted that there were three areas outstanding:

- Cyber security training for members – a new provider was being sought as it was felt that the current training provider did not pitch the training at board member level
- The lessons learned report needed to be circulated to the full Authority
- Data security and protection toolkit (DSPT) was an agenda item so would be discussed later in the meeting.

3.2. The committee noted the progress on actions from previous meetings and the updates presented at the meeting.

4. Digital programme update

4.1. The digital programme update was presented by the Chief Information Officer (CIO). It was noted that data quality issues identified at an earlier meeting had been resolved, tests were being carried out and third-party system providers were currently looking at their systems and would be deployed these over time.

4.2. Members were informed that training transition meetings were being held with HFEA staff on a weekly basis to ensure a smooth transition when the external consultants left the organisation.

4.3. Members commented that they felt more comfortable that knowledge was captured by being documented. This also mitigated the potential risk of relying on a small number of core staff due to the size of the HFEA.

4.4. It was noted that the options considered for the cutover period was for the end of March, end of April and end of May which were consistent with the public message that we would launch PRISM no earlier than 31 March and no later than 31 May. During discussion, it was observed that cutover in May would cost the same as going live in April and it would present the least level of risk. The end of May date was therefore the recommended and preferred option.

4.5. Communication had been shared with stakeholders including clinics and suppliers stating that the cutover would be in the month of May.

4.6. Members were advised that the PRISM system had been audited and the outcome from the audit would be presented to the executive by the Auditors at the end of March.

4.7. Feedback had been received around the communications plan. The Internal Auditor commented that nothing fundamental had been flagged up, but noted that it was a short specific audit, focused around pre-launch readiness.

4.8. In response to a question, members were advised that a comprehensive lessons' learned document was yet to be drawn up.

4.9. Members asked about the engagement from clinics and how extensive this was. It was noted that because the launch date had been announced clinics were now more focused and this led to their re-engagement.

Decision

4.10. Members welcomed the progress to date.

5. 2020/21 Internal audit delivery update and 2021/22 proposed internal audit plan

5.1. The Chair invited the Internal Auditor to present the 2020/21 internal audit delivery update and proposed internal audit plan for 2021/22.

5.2. The Internal Auditor commented that there was one revision to the audit plan which was to remove the office move item. The committee ratified this.

5.3. There were two reports presented at the meeting

- developing a virtual inspection process
- Accounts payable/ accounts receivable.

Members were informed that both reports had been given a substantial assurance rating.

5.4. The committee welcomed this and commented that receiving two reports at the same meeting and both with substantial ratings was a very good outcome and congratulated all involved.

5.5. Members were advised that in relation to the digital programme, in particular PRISM, being heavily reliant on an individual remained a risk that needed to be managed. It was important that the standard operating procedures (SOP) were kept up to date and this was set out in the 2019-2020 recommendations.

5.6. Members asked if the Department of Health and Social Care (DHSC) could assist with large digital projects. The Internal Auditor responded that it was possible and the GIAA could also offer support as they had some resources to cater for such projects. Members commented that, where possible, large projects needed to be avoided in small organisations or ways found where external expertise could be easily identified.

5.7. In response to a question on the longer-term plan for inspections, the Chief Executive stated that we were required by law to inspect licensed premises within a 2-year period but during the pandemic we were unable to do this. A modified risk based approach using a desk based analysis and virtual technology had been developed. Post the pandemic, we would have to follow the letter of the law and physically inspect all licensed premises but we are looking to introduce a hybrid model which would include having the pre-inspection desk based phase. This modified approach would mean less time would be spent on site. In the longer term it might be possible to change the law, but a hybrid model would ensure that we are complying with the Act.

5.8. Members were also advised that a questionnaire was being developed and would be sent to clinics who had taken part in desk-based inspections during the pandemic to gather their views.

5.9. In terms of the release of data, Members asked if this was also around security of data or specifically publication of data. The Internal Auditor responded that it was around the publication of data and to ensure that the HFEA was compliant with the requirements of the Act.

5.10. The Chief Executive commented that we had no concerns around the security of data and to ensure that this remained the case, we were adding extra resources to the team that managed the release of Register information.

5.11. The committee was asked for their views about the new updated format of the audit plan. Members were supportive noting that it was easier to follow. The Director of Finance and Resources commented that the HFEA would improve at feeding back to surveys.

5.12. The Internal Auditor commented on the internal audit plan for 2021/22 and presented the areas of activity that would be audited. Members were advised that some areas had been excluded from the plan following discussion with stakeholders.

5.13. Members commented that preparedness for opening the register was a big risk and wanted to know why it was excluded. The Internal Auditor responded that it was in the pipeline and would be reviewed mid-year with the senior management team (SMT).

5.14. The Chair agreed that this should be kept under review as Members were very interested.

5.15. Members asked about having a short audit on PRISM and benefits realisation. The Director of Finance and Resources commented that any additional days would incur an additional cost as all audit days had been allocated.

5.16. Following a discussion, the Chair agreed that it could be left in the pipeline and see if it could be accommodated later on in the year.

Decision

5.17. The committee ratified the removal of the office move from the audit plan.

5.18. Members noted the 20/21 Internal Audit update.

5.19. Members ratified the proposed plan for 2021/22 and associated documentation which were the 2021/22 Internal Audit Charter and the 2021/22 Internal Audit Memorandum of Understanding.

6. Implementation of recommendations

6.1. The Head of Finance presented the summary of the audit recommendations.

6.2. It was proposed that the payables and receivables item should come off the list as all recommendations had been implemented.

6.3. The risk and management of capabilities was outstanding, the Head of Human Resources would be asked to provide an update.

6.4. Members asked if the business continuity (BC) training was referring to refresher training. The CIO responded that this was the case but where we had new staff it might be their first time for the BC training.

6.5. In response to a question, the Chief Executive commented that SOPs were updated regularly across the organisation and while there might be occasional lapses there was nothing structural.

Decision

6.6. Members noted the progress of the recommendations and ratified the removal of the payables and receivables item from the list of recommendations.

7. External audit interim feedback

7.1. The External Auditor gave an update to the committee.

7.2. Members were advised that the initial audit work had been completed and there was nothing to bring to their attention as everything seemed to be in order.

7.3. Regarding cyber security training for members, the external auditor stated that he would circulate a NAO guidance document relating to this to the Chair and the Governance Manager.

Decision

7.4. Members noted the update.

8. Resilience, business continuity management, cyber security training

8.1. The Chair invited the Chief Information Officer (CIO) to present this item to the committee. The CIO gave a synopsis of the IT infrastructure and software development and commented that laptop replacements would be deployed shortly in line with our refresh programme.

8.2. Members were also advised that following a lengthy and very detailed piece of work by the Register team, the Choose a Fertility Clinic (CaFC) section on the website was refreshed in February 2021.

8.3. It was noted that demand on the opening the register team had increased significantly in recent months, but to ease this, the team would be strengthened by recruiting to a fixed term post to help reduce waiting times for applicants.

8.4. Members were informed that the Data Security and Protection Toolkit (DSPT) interim submission was made in February 2021. The final submission was due in June 2021 and we were expecting to meet 35 out of 37 requirements but the submission would be categorised as not met.

8.5. Members commented that the members training on data security and protection needed to be pushed out as soon as possible.

8.6. The Director of Finance and Resources commented that the BC plan was running well but we needed to focus on the 'softer' business continuity points.

8.7. It was noted that there would be continued discussions with NHSX about flexibility.

Decision

8.8. Members noted this item.

9. Strategic risk register

9.1. The Risk and Business Planning Manager presented this item to the committee. It was noted that C2 - board capability risk level had been reduced. The reduction at this time reflected the improved position in board member recruitment.

9.2. Members were reminded that the risk management policy was brought to them in December 2018 and the risk appetite statement was last brought in June 2020. The Risk and Business Planning Manager noted there was the intention to review the whole HFEA risk management approach and bring the revised policy back to the committee at its October meeting before confirming the risk appetite statement with the Authority when the risk register goes to them in November 2021. This would ensure an embedded approach.

9.3. Members suggested that a dynamic risk register should be considered as experience dictated that it offered more value. Members also asked if we were identifying too many risks rather than concentrating on specifically strategic ones.

9.4. The Chief Executive responded that with a new Chair and Authority Members joining it was a good time to review both the approach and the register prior to it going to the November Authority meeting.

9.5. The Director of Finance and Resources suggested that we could utilise the approach used for operational risk management and present the top three organisational risks. Members commented that there was still a need to focus on strategic risks.

9.6. The Risk and Business Planning Manager commented further on the register. It was noted that

- OM1 - operating model was a new risk and so it was still developing and bedding in
- PI - positioning and influencing risk had been reduced to reflect that this was no longer as big a threat as it was previously
- CV1 - coronavirus was also reduced, as our revised regulatory approach was working well.

9.7. In response to a question, it was noted that the pressure on the opening the register system was currently being managed as a live issue, and the related risk was reflected under the information risk (I1).

9.8. Members commented that in relation to board capability, the key concern was knowledge management, it was important to capture knowledge to ensure consistency in decision making. Legacy planning at SMT level also needed to be taken into consideration. This risk could be reframed to reflect this.

9.9. Members suggested that risk of not effectively managing and capitalising on stakeholder engagement could be reflected under OM1 as this related to the impact of Covid-19 on the sector.

9.10. Members asked if DNA testing was part of our legislative 'wish' should the DHSC decide to reopen the Act in the future. The Chief Executive responded that it depended on what the government wanted to do, but as things currently stood, we did not regulate this, but we would continue to work with DNA testing providers informally to provide information to users. The Chair requested that a paper on confidentiality and DNA testing should be taken to the Authority as it needed to be revisited.

9.11. In response to a question on the difference of views of inspectors and the hybrid inspection system, the Chief Executive commented that we continued to work towards an operating consensus with inspectors about the required detail of reviews and we would update the committee.

Decision

9.12. Members noted the strategic risk register.

10. Policies

Public interest disclosure (whistle blowing) policy

10.1. The Head of Finance introduced this item. It was noted that 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.

10.2. Members commented that whilst working remotely it was difficult to whistle blow. Members also asked how easy it was for staff to whistle blow since everything needed to be sent via email which did not guarantee confidentiality.

10.3. Members suggested that an external contact point/external email address could be pursued so that it was independent of the HFEA and could give staff the confidence to report any wrongdoing.

10.4. Members commented that the inclusion of the Nolan principles in the policy was a very good move.

Decision

10.5. Members approved the policy, subject to the review of the inclusion of an external contact point.

Counter fraud strategy

10.6. The Head of Finance presented the counter fraud strategy with the suggested updates highlighted in the report.

Decision

10.7. Members approved the strategy with the additions.

Counter-fraud and anti-theft policy

10.8. The Head of Finance presented this item. It was noted that the counter fraud and anti-theft policy was implemented to ensure people working for the HFEA were aware that fraud could exist and how to respond if fraud was suspected.

10.9. Members welcomed the policy and commented that it should be specified in the policy how often it would be brought to committee.

Decision

10.10. Subject to the inclusion of the timeline, the committee approved the policy.

11. AGC forward plan

11.1. The Head of Finance presented this item.

11.2. The Director of Finance and Resources confirmed that the annual governance statement would be circulated by the end of March 2021.

Decision

11.3. Members noted the current position of the forward plan.

12. Gift and hospitality

12.1. The register of gifts and hospitality was presented to the committee. There were no changes.

13. Whistle blowing and fraud

13.1. There were no cases of whistle blowing or fraud to report.

14. Contracts and procurement

14.1. There were no new contracts or procurements to report.

15. Any other business

15.1. Members were informed of a programme on BBC2 on 16 March 2021 on donor conception, which included information about our opening the register service. The programme was part of a 3-part documentary series.

15.2. In response to a question about the plan on returning to the office, it was noted that the new office was ready for occupation but in compliance with the government's regulations, the earliest date staff would be expected to return would be 21 June 2021. In the meantime, we would work from home where possible.

15.3. The Chair requested that members and staff views on returning to face-to-face AGC meetings should be emailed to her, but the Chair's view was that meetings could remain virtual.

Chair's signature

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

Signature

Chair: Anita Bharucha

Date: 22 June 2021

AGC Matters Arising

Details about this paper

Area(s) of strategy this paper relates to:	The best care – effective and ethical care for everyone The right information – to ensure that people can access the right information at the right time Shaping the future – to embrace and engage with changes in the law, science, and society

Meeting	Audit and Governance Committee		
Agenda item	3		
Paper number	HFEA (16/03/2021) MA		
Meeting date	22 June 2021		
Author	Morounke Akingbola (Head of Finance)		
Output:			
For information or decision?	For information		
Recommendation	To note and comment on the updates shown for each item.		
Resource implications	To be updated and reviewed at each AGC		
Implementation date	2021/22 business year		
Communication(s)			
Organisational risk	☐ Low	**X** Medium	☐ High

ACTION	RESPONSIBILITY	DUE DATE	PROGRESS TO DATE
Matters Arising from the Audit and Governance Committee – actions from 6 October 2020			
13.4 Cyber security training to be confirmed to members	Head of Finance	Dec-20	**Update** – training was provided using the Astute training platform. Reminder to be sent to members before the Christmas break.
Matters Arising from the Audit and Governance Committee – actions from 8 December 2020			
8.9 Lessons learned report to be tabled at an Authority meeting	Director of Finance and Resources	June-21	**Update –** To be circulated outside of the meeting
10.6 Data Security and protection toolkit (DSPT) self-assessment progress update and sign-off ahead of its submission	Chief Information Officer	On-going	**Update –** To be provided during meeting.

SIRO Report

Strategic delivery:	☒ Safe, ethical, effective treatment	☐ Consistent outcomes and support	☐ Improving standards through intelligence
Details:			
Meeting	Audit and Governance Committee		
Agenda item	7		
Paper number	HFEA (22/06/2021) RS		
Meeting date	22 June 2021		
Author	Richard Sydee, Director of Resources		
Output:			
For information or decision?	For information		
Recommendation	N/A		
Resource implications	N/A		
Implementation date	N/A		
Communication(s)	N/A		
Organisational risk	☐ Low	☒ Medium	☐ High
Annexes			

1. Background

1.1. The Senior Information Risk Officer's (SIRO) holds responsibility to manage the strategic information risks that may impinge on our ability to meet corporate objectives, providing oversight and assurance to the Executive and Authority of the HFEA. It is a Cabinet Office (CO) requirement that Boards receive regular assurance about information risk management. This provides for good governance, ensures that the Board is involved in information assurance and forms part the consideration of the Annual Governance Statement (AGS).

1.2. This report is my annual report to the Accounting Officer and AGC.

1.3. The Security Policy Framework (SPF) provides a suitable format for the HFEA's report. ALBs are also asked to assess themselves and report against the 10 Steps to Cyber Security, the guidance issued as part of the Government's Cyber Security strategy. The HFEA has made such an assessment and recorded relevant actions and risks as part of the operational risk register, which is reviewed monthly by the HFEA Management Group.

2. Report

2.1. The HFEA routinely assess the risks to information management across the organisation, through its assessment of the risk of data loss, cyber security and the inclusion of guidance on creating and managing records throughout its Standard Operating Procedures (SOPS) and policies.

2.2. The HFEA has historically held and processed personal data and records and maintained robust controls and security protocols around all data relating to fertility treatments, which it is required to hold under the HFE Act.

2.3. In recent years we have also responded to changes in legislation relating to the broader personal data we hold on our staff, clinic staff and members of the pubic who may have contacted us. We have introduced several changes to our policies and procedures to ensure we comply with the General Data Protection Regulation and the Data Protection Act.

2.4. Throughout the year we undertake scheduled activity to ensure we comply with our policies; this work Is overseen by the HFEA's Information Governance Manager who makes periodic reports to the Corporate Management Group. In particular:

- During the year we have finalised and published a revised document retention policy.
- We continue to regularly reviews our Information asset register, ensuring all assets have owners who are reviewing the assets held, there purpose and use. We have protocols to ensure documents that have reached the end of their retention period are reviewed and either deleted or the retention period extended.
- We have updated the information risk training we are using and have made this mandatory across the organisation

2.5. This provides an overview of our approach to RM and specifically the roles and responsibilities of staff across the organisation as well as our approach to record retention and deletion.

2.6. We continue to review our process for assessing our approach to capturing the level of information risk and out=r tolerance of it. Given the size of the HFEA there is limited resource to provide continuous oversight of this issue, as such our approach is proportionate and looks to embed the consideration of information risks within the broader assessment of organisational risks.

2.7. Overall, we have a low tolerance of risk for information on our Register database, that which falls within the auspices of GDPR and is commercially sensitive or business critical. The focus of our resource will continue to be the secure and compliant storage of these records.

2.8. In terms of the security of our data the HFEA has appropriate cyber security polices in place. AGC regularly receive updates on cyber security and I am assured that the HFEA's approach to cyber security provides significant protection of our information assets and that there is active monitoring of cyber security with appropriate action taken to improve the level of protection against new and emerging cyber threats.

2.9. I have considered the HFEAs compliance with the mandatory requirements set out in the SPF, see Security policy framework - Publications - GOV.UK. The requirements were last updated in July 2014 and focus on eight areas (governance, culture, risk management, information, technology, personnel, physical security, responding to incidents) with three types of consideration for each of those (information, physical and people). The requirements have been applied proportionately and matched to the HFEA's organisational risks. Not all of the areas apply to the HFEA. This is contained at Appendix A to this document.

2.10. In line with the Office of the Government SIRO handbook I have also considered a number of the factors that underpin the management of the HFEA's information risks.

- I believe the HFEA have an effective Information Governance framework in place and that the HFEA complies with all relevant regulatory, statutory and organisation information security policies and standards.
- I am satisfied that the HFEA has introduced and maintains processes to ensure staff are aware of the need for information assurance and the risks affecting corporate information.
- The HFEA has appropriate and proportionate security controls in place relating to records and data and that these are regularly assessed.

2.11. In conclusion I believe the HFEA has progressed in its approach to data, information and records management over the past year and is in a stronger position in terms of its governance in this area as a consequence. As SIRO I believe the HFEA takes issues relating to information risk seriously and has appropriate processes in place to assess and minimise these risks. We will continue to maintain and improve processes over the coming year and ensure we consider how we can maximise the use of our information as a business asset.

Annex A - Assessment of the HFEAs compliance with the Security Policy Framework 2014 (As at 31 March 2021)

	Mandatory Requirement	Compliance	Further actions required
1	Departments and Agencies must establish an appropriate security organisation (suitably staffed and trained) with clear lines of responsibility and accountability at all levels of the organisation. This must include a Board-level lead with authority to influence investment decisions and agree the organisation's overall approach to security.	Director of Resources is SIRO, Chief Information Officer has day to day responsibility of information security.	Ongoing review and refresher training as required.
2	Departments and Agencies must: * Adopt a holistic risk management approach covering all areas of protective security across their organisation. * Develop their own security policies, tailoring the standards and guidelines set out in this framework to the particular business needs, threat profile and risk appetite of their organisation and its delivery partners.	Risks identified as part of routine operational and strategic risk management as well as detailed on the information asset register Policies are in place and reviewed annually.	Ongoing review and development of the information asset register.
3	Departments and Agencies must ensure that all staff are aware of Departmental security policies and understand their personal responsibilities for safeguarding assets and the potential consequences of breaching security rules.	All staff and Authority members are informed of policies and given guidance. Annual training is undertaken by all	Ongoing reminders and awareness raising with staff.

		through Civil Service Learning.	
4	Departments and Agencies must have robust and well tested policies, procedures and management arrangements in place to respond to, investigate and recover from security incidents or other disruptions to core business.	System in place for detecting security breaches and business continuity arrangements in place.	None.
5	Departments and Agencies must have an effective system of assurance in place to satisfy their Accounting Officer / Head of Department and Management Board that the organisation's security arrangements are fit for purpose, that information risks are appropriately managed, and that any significant control weaknesses are explicitly acknowledged and regularly reviewed.	System in place and SIRO reports annually - any weaknesses identified in Governance Statement (none). Response to GDPR and Records management audits during 2018/19 have also been reflected in HFEA processes	None.
6	Departments and Agencies must have an information security policy setting out how they and any delivery partners and suppliers will protect any information assets they hold, store or process (including electronic and paper formats and online services) to prevent unauthorised access, disclosure or loss. The policies and procedures must be regularly reviewed to ensure currency.	Policies and procedures are in place and reviewed annually.	None.
7	Departments and Agencies must ensure that information assets are valued, handled, shared and protected in line with the standards and procedures set out in the Government Security Classifications	The HFEA's assets are all classified OFFICIAL and are appropriately controlled.	None.

	Policy (including any special handling arrangements) and the associated technical guidance supporting this framework.		
8	All ICT systems that handle, store and process HMG classified information or business critical data, or that are interconnected to cross-government networks or services (e.g. the Public Services Network, PSN), must undergo a formal risk assessment to identify and understand relevant technical risks; and must undergo a proportionate accreditation process to ensure that the risks to the confidentiality, integrity and availability of the data, system and/or service are properly managed.	ICT systems are risk assessed as part of the overall operational risk register. IT security was reviewed by Internal Audit in 2017/18	None
9	Departments and Agencies must put in place an appropriate range of technical controls for all ICT systems, proportionate to the value, importance and sensitivity of the information held and the requirements of any interconnected systems.	Patching and firewalls in place. Assurance reports received and reviewed regularly with suppliers. Portable devices and removable media is secured.	None.
10	Departments and Agencies must implement appropriate procedural controls for all ICT (or paper-based) systems or services to prevent unauthorised access and modification, or misuse by authorised users.	Policies and staff induction in place, to clarify proper use and implications of breaches.	None.
11	Departments and Agencies must ensure that the security arrangements among their wider family of delivery partners and third-	Contracts include required conditions and where appropriate third	None.

	party suppliers are appropriate to the information concerned and the level of risk to the parent organisation. This must include appropriate governance and management arrangements to manage risk, monitor compliance and respond effectively to any incidents. Any site where third party suppliers manage assets at SECRET or above must be accredited to List X standards.	parties are given copies of the HFEA's system policies. Changes to arrangements and incident monitoring and results are reviewed at quarterly meetings with suppliers.	
12	Departments and Agencies must have clear policies and processes for reporting, managing and resolving Information Security Breaches and ICT security incidents.	Policies have been revised and are in place.	None.
13	Departments must ensure that personnel security risks are effectively managed by applying rigorous recruitment controls, and a proportionate and robust personnel security regime that determines what other checks (e.g. national security vetting) and ongoing personnel security controls should be applied.	Recruitment and references provide assurance. No vetting in place as very little sensitive data.	None.
14	Departments and Agencies must have in place an appropriate level of ongoing personnel security management, including formal reviews of national security vetting clearances, and arrangements for vetted staff to report changes in circumstances that might be relevant to their suitability to hold a security clearance.	N/a.	
15	Departments must make provision for an internal appeal process for existing employees wishing to challenge National Security Vetting	N/a.	

	decisions and inform Cabinet Office Government Security Secretariat should an individual initiate a legal challenge against a National Security Vetting decision.		
16	Departments and Agencies must undertake regular security risk assessments for all sites in their estate and put in place appropriate physical security controls to prevent, detect and respond to security incidents.	Assessment and sufficient controls provided by building management.	None.
17	Departments and Agencies must implement appropriate internal security controls to ensure that critical, sensitive or classified assets are protected against both surreptitious and forced attack and are only available to those with a genuine “need to know". Physical security measures must be proportionate to the level of threat, integrated with other protective security controls, and applied on the basis of the “defence in depth" principle.	Visitor and entry controls provided by building management. Lockable furniture provided for storage. Clear desk and clear screen requirements reinforced through training, checks and reminders.	None.
18	Departments and Agencies must put in place appropriate physical security controls to prevent unauthorised access to their estate, reduce the vulnerability of establishments to terrorism or other physical attacks, and facilitate a quick and effective response to security incidents. Selected controls must be proportionate to the level of threat, appropriate to the needs of the business and based on the “defence in depth" principle.	Sufficient controls around access and mail provided by building management.	None.

19	Departments and Agencies must ensure that all establishments in their estate put in place effective and well tested arrangements to respond to physical security incidents, including appropriate contingency plans and the ability to immediately implement additional security controls following a rise in the Government Response Level.	Building management provide the lead on incidents. HFEA have contingency plans in place that are reviewed annually, and incident management processes were utilised in 2018 in relation to a power outage	None.
20	Departments and Agencies must be resilient in the face of physical security incidents, including terrorist attacks, applying identified security measures, and implementing incident management contingency arrangements and plans with immediate effect following a change to the Government Response Level.	Building management provide the lead on incidents. HFEA have contingency plans in place that are reviewed annually, and incident management processes were utilised in 2018 in relation to a power outage	

Strategic risk register 2020-2024

Details about this paper

Area(s) of strategy this paper relates to:	The best care – effective and ethical care for everyone The right information – to ensure that people can access the right information at the right time Shaping the future – to embrace and engage with changes in the law, science and society
Meeting:	Audit and Governance Committee
Agenda item:	10
Paper number:	HFEA (22/06/2021) HC
Meeting date:	22 June 2021
Author:	Helen Crutcher, Risk and Business Planning Manager Paula Robinson, Head of Planning and Governance
Annexes	Annex 1: Strategic risk register 2020-2024

Output from this paper

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:	Ongoing
Communication(s):	Feedback from AGC will inform the next SMT review in July.
Organisational risk:	Medium

1. Latest reviews

1.1. Authority received the Strategic Risk Register at its meeting on 12 May. Authority members raised some interesting reflections on the strategic risk register (SRR) and risk approaches more generally.

1.2. One such reflection was a challenge about the nature of some of the risks reflected in the register and whether some of this was hypothetical rather than real risk, ie, causes that could theoretically occur rather than those which were apparent and that posed risks.

1.3. SMT reviewed the register at its meeting on 9 June 2021. SMT reviewed all risks, controls and scores. Following the comments made by Authority, you will note that a number of causes have been either reframed, to reflect the true risks, or removed entirely, where these were found to be more theoretical.

1.4. SMT's comments are summarised in the commentary for each risk and at the end of the register, which is attached at Annex 1. The annex also includes a graphical overview of residual risk scores plotted against risk tolerances.

1.5. One of the ten risks is above tolerance.

2. New framing of the C2 risk

2.1. In May, the C2 risk was reframed to include concerns of AGC and Board Members about the management of risk related to senior executive appointments as well as the Member-related risks. Discussions are underway with the Chair about management of these added risks and a key area of focus over the coming months will be developing explicit succession plans.

3. Progress with risk management review

3.1. Results of early conversations with partner organisations:

- Since the last AGC we've had conversations with Catharine and one of her colleagues at the Legal Services Board who have kindly shared their risk approach.
- We've also discussed risk assurance mapping with the joint Director of Finance and Resources, who noted that the HTA now review this quarterly in parallel to discussions of their SRR.

3.2. We anticipate that the review over the summer is likely to result in a more substantial overhaul of the structure and content of the SRR. However, due to resourcing, that has not yet begun. We are also keen not to lose aspects that worked with the current approach over a number of years. A priority will be focusing on creating a supportive risk culture around any changes, and an ongoing improvement plan, rather than simply revising documentation.

3.3. High-level review plan for the coming months

June	Review of best practice guidance and other organisational approaches including Orange Book and risk improvement groups (DHSC and Cross-government)
July	Review of operational risk management practices and identification of weaknesses

August	Design of rolling improvement plans Redrafting of policy and processes to begin
September	Revised draft of risk policy/strategy completed
October	Presentation of revisions to approach and ongoing plans to AGC
November	Agreement of risk appetite with Authority alongside their periodic review of the risk register.

4. Recommendation

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

Latest review date – 14/06/2021

Strategic risk register 2020-2024

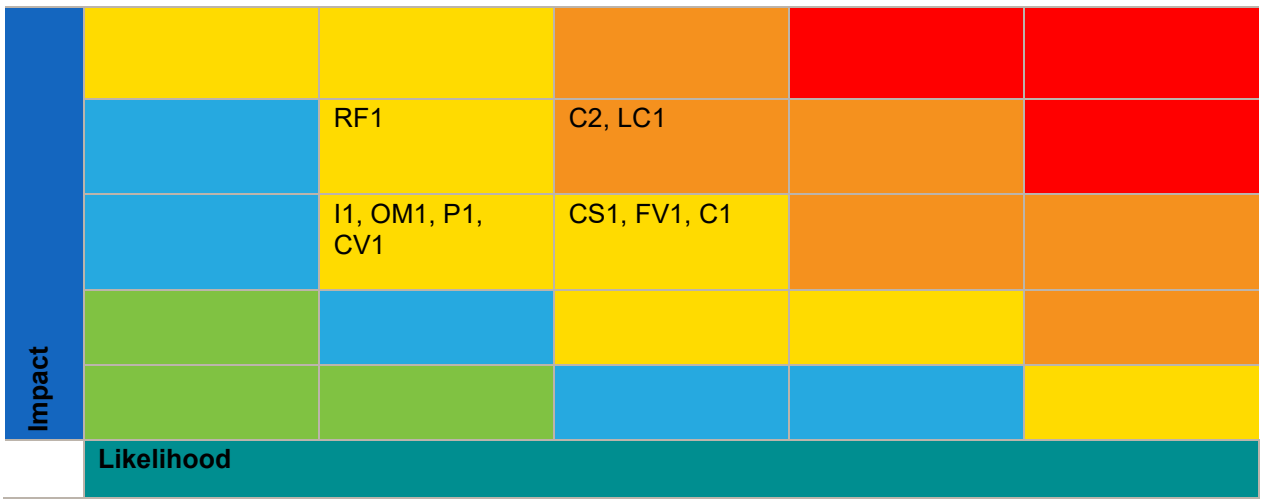
Risk summary: high to low residual risks

Risk ID	Strategy link	Residual risk	Status	Trend*
C2: Board capability	Generic risk – whole strategy	**12 – High**	Above tolerance	⇔⇧⇔⇔
LC1: Legal challenge	Generic risk – whole strategy	**12 – High**	At tolerance	⇔⇔⇔⇧
FV1: Financial viability	Generic risk – whole strategy	**9 – Medium**	At tolerance	⇔⇔⇔⇔
C1: Capability	Generic risk – whole strategy	**9 – Medium**	Below tolerance	⇔⇔⇔⇔
CS1: Cyber security	Generic risk – whole strategy	**9 – Medium**	At tolerance	⇔⇔⇔⇔
RF1 – Regulatory framework	The best care (and whole strategy)	**8 – Medium**	At tolerance	⇔⇔⇔⇔
OM1: Operating Model	Whole strategy	**6 – Medium**	At tolerance	⇔⇔⇔⇔
I1 – Information provision	The right information	**6 – Medium**	Below tolerance	⇔⇔⇔⇔
P1 – Positioning and influencing	Shaping the future (and whole strategy)	**6 – Medium**	Below tolerance	⇔⇔⇔⇔
CV1 - Coronavirus	Whole strategy	**6 – Medium**	Below tolerance	⇔⇔⇔⇔

*This column tracks the four most recent reviews by AGC, SMT or the Authority (eg,⇧⇔⇩⇔).

Recent review points: AGC 16 March ⇨ SMT 19 April ⇨ Authority 12 May ⇨ SMT 9 June

Summary risk profile – residual risks plotted against each other:



RF1: There is a risk that the regulatory framework in which the HFEA operates is overtaken by developments and becomes not fit for purpose.

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
3	5	15	**2**	**4**	**8 - Medium**
Tolerance threshold:					**8 - Medium**
Status: **At tolerance**					

Risk area	Risk owner	Links to which strategic objectives?	Trend
Regulatory framework RF1: Responsive and safe regulation	Rachel Cutting, Director of Compliance and Information	The best care and whole strategy	⇔⇔⇔⇔

Commentary

As a regulator, we are by nature removed from the care and developments being offered in clinics and we must rely on our regulatory framework to provide sufficient powers to assure the public that treatment and research are safe and ethical.

The result of not having an effective regulatory framework could be significant. The worst case of this risk would be us being without appropriate powers or ability to intervene, and patients being at risk, or not having access to treatment options that should be available to them in a safe and effective way.

We reworked our inspection methodology as a result of Covid-19, to undertake remote and hybrid inspections to reduce risk. As at June 2021, inspectors are returning to on-site inspections, and the aim is to reach a balanced steady state between desk-based assessments and on-site inspections, balancing workloads and risk.

There is a higher resource requirement for these new processes, and we are keeping this under close review to ensure that it remains appropriate. There is still a degree of risk – for example the licence extensions implemented in 2020/21 mean there is an inspection scheduling issue in January 2022, with a bottleneck of inspections due at that point. To manage this we will need to continue to breach the two yearly visit rule for some clinics, and extend licences where this is possible.

SMT agreed in March and June 2021 that although this is a new source of risk for RF1, this does not yet suggest the overall risk score has increased, but we will continue to keep this under close review.

Causes / sources	Controls	Timescale / owner of control(s)
We don't have powers in some of the areas where there are or will be changes affecting the	We are strengthening or seeking to build connections with relevant partners who do have powers in such areas (for instance, the CMA in relation to pricing of treatments).	In progress - Clare Ettinghausen

Causes / sources	Controls	Timescale / owner of control(s)
fertility sector (for instance artificial intelligence).	We take external legal advice as relevant where developments are outside of our direct remit (eg, on an incidence of AI technology being used in the fertility sector) and utilise this to establish our legal/regulatory position. We are analysing where there are gaps in our regulatory powers so that we may be able to make a case for further powers if these are necessary, whenever these are next reviewed.	Ongoing - Catherine Drennan In progress - Laura Riley, Joanne Anton, Catherine Drennan
Developments occur which our regulatory tools, systems and interventions have not been designed to address and they are unable to adapt to.	Regular review processes for all regulatory tools such as: • Code of Practice. • Compliance and enforcement policy (Final draft of revised policy signed off by Authority in March 2021 and coming into effect in June 2021) • Licensing SOPs and decision trees To enable us to revise these and prevent them from becoming ineffective or outdated. Regular liaison with DHSC and other health regulators to raise issues.	In place, next update 2021 – Laura Riley, Joanne Anton In place but a revised version of the policy to be launched, subject to Authority agreement, in June 2021– Catherine Drennan, Rachel Cutting In place and review ongoing – Paula Robinson In place - Peter Thompson
The revised inspection approach (including fully remote and hybrid inspections due to Covid-19, introduced November 2020) requires greater resources from the inspection team. This will affect ongoing delivery if it continues for a sustained period. Note: risk cause arises from control under CV1.	Reviewing the new way of working and inspection approach as this continues to be embedded. Moving towards a steady state balance between desk-based elements and on-site inspections. Compliance management in discussion with the wider Inspection team to ensure that scrutiny is at the correct level and inspections are 'right sized' in accordance with revised methodology. Clear communication to the inspection team about appropriate level of scrutiny. Continued extensions to some licences where appropriate (ie, low risk clinics with good compliance) to manage the pressure on inspection delivery workload.	In progress – Sharon Fensome Rimmer, Rachel Cutting

Causes / sources	Controls	Timescale / owner of control(s)
Some changes can be very fast meaning our understanding of the implications is limited, affecting our ability to adequately prepare, respond and take a nuanced approach	We cannot control the rate of change, but we can make sure we are aware of likely changes and make our response as timely as possible by: • Annual horizon scanning at SCAAC • maintaining links with key stakeholders including other professional organisations and the licensed centres panel to get a sense of changes they are experiencing or have early sight of. We necessarily have to wait for some changes to be clearer in order to take an effective regulatory position. However, we may choose to take a staged approach when changes are emerging, issuing quick responses such as a Chair's letter, Alert or change to General Directions to address immediate regulatory needs, before strengthening our position with further guidance or regulatory updates.	In place – Laura Riley, Joanne Anton In place - Peter Thompson
We have limited capacity, which may reduce our ability to respond quickly to new work, since we may need to review and stop doing something else.	Monthly opportunity for reprioritising at CMG when new work arises and weekly SMT meetings for more pressing decisions. Any reprioritisation of significant Strategy work would be discussed with the Authority.	In place – Peter Thompson
Developments occur in areas where we have a lack of staffing expertise or capability.	As developments occur, Heads consider what the gaps are in our expertise and whether there is training available to our staff. If a specific skills gap was identified in relation to a new development, we could consider whether it is appropriate or possible to bring in resource from outside, for instance by employing someone temporarily or sharing skills with other organisations.	Ongoing - Relevant Head/Director with Yvonne Akinmodun
RITA (the register information team app – used to review submissions to the Register) has been built but some reporting issues still need to be resolved, If it is not completed in a timely way, we may not effectively use data and ensure our regulatory actions are based on the best and most current information.	If RITA is not completed in a timely way, the Register and OTR team will still be able to use manual workarounds to get access to the information they need to support clinics and / or to provide information to support our regulatory work. although these workarounds will result in a substantial delay to responding to an OTR or providing clinic support. If additional development work is required to complete RITA phase 1 (essential functionality) development in a timely way, we will consider options for providing the necessary resource. However, this control may impact on our ability to support or develop other internal applications.	Ongoing – Dan Howard Under review as delivery continues - Dan

Causes / sources	Controls	Timescale / owner of control(s)
We don't hold all of the data from the sector (beyond inspection or Register data) to inform our interventions, for instance on add-ons.	As part of planning and delivering the add-ons project we have looked at the evidence available and considered whether we can access other information if we do not have this already. We revise our approach on inspection where relevant, to ensure that the right information is available (for instance, launching an add-ons audit tool). Process to be established for reviewing data on the Register and adding fields when required.	In place - Laura Riley Audit tool launched in clinics from Autumn 2020 - Rachel Cutting Within 2021/2022 business year - Dan Howard
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
DHSC - If there was a review of our regulatory powers, there would be a strong interdependency with the Department of Health and Social Care.	Early engagement with the Department to ensure that they are aware of HFEA position in relation to any future review of the legislation. Provided a considered response to the Department's storage consent consultation to give the HFEA position.	Ongoing - Peter Thompson

I1: There is a risk that HFEA becomes an ineffective information provider, jeopardising our ability to improve quality of care and make the right information available to people.

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	3	12 - High	**2**	**3**	**6- Medium**
Tolerance threshold:					**8- Medium**
Status: **Below tolerance**					

Risk area	**Risk owner**	**Links to which strategic objectives?**	**Trend**
Information provision I1: delivering data and knowledge	Clare Ettinghausen, Director of Strategy and Corporate Affairs	The right information	⇔⇔⇔⇔

Commentary
Information provision is a key part of our statutory duties and is fundamental to us being able to regulate effectively. We provide information to the public, patients, partners, donors, the donor conceived, their families and clinics alike. If we are not seen as relevant then we risk our information not being used, which in turn may affect the quality of care, outcomes and options available to those involved in treatment. In October 2020, the Opening the Register service reopened after being paused since clinics shut down due to Covid-19. Due to this pause, we received an influx of applications which means we are unable to meet our usual KPI for completing responses for a period. We are managing this carefully as a live issue, to ensure that applicants receive accurate data and effective support as quickly as we are able, with a focus on continuing to provide a quality, effective service. Ongoing communication with applicants and centres has been clear, to ensure they understand, and we manage expectations. We have recruited extra resource to manage the backlog but the impact of this will take some time to resolve the issue and reduce the ongoing risk.

Causes / sources	**Controls**	**Status / timescale / owner**
People don't find us/our information, meaning we are unable to get clear and unbiased information to patients, donors and others.	Knowledge of key searches and work to improve search engine optimisation to ensure that we will be found. We have a rolling bi-annual cycle to review website content and can revise website content to ensure this is optimised for search if necessary. We undertake activities to raise awareness of our information, such as using social and traditional media. We maintain connections with other organisations to ensure that others link to us appropriately, and so we increase the chance of people finding us.	In place and ongoing - Jo Triggs

Causes / sources	Controls	Status / timescale / owner
We aren't in the places that people look for information meaning they do not find us. In some cases, this is because we have decided not to be, for instance on some social media platforms.	We are developing relationships with key influencers to ensure that we have an indirect presence on social media or forums.	In place and ongoing - Jo Triggs
We do not have effective relationships with key strategic stakeholders.	Ensure a strategic stakeholder engagement plan is agreed and revisited frequently. Stakeholder engagement plans considered as part of project planning to ensure this is effective.	Early work done but development needed, future control – Clare Ettinghausen Ongoing – Paula Robinson
We have more competition to get information out to people. For instance, other companies have set up their own clinic comparison sites and clinics post their own data.	Ensure we maximise the information on our website and the unique features of our clinic inspection information and patient ratings. Clinics are encouraged to ask patients to use the HFEA patient rating system. We have optimised Choose a Fertility Clinic so that it is one of the top sites that patients will find when searching online. Review our information and distribution mechanisms on an ongoing basis to ensure relevance.	In place and ongoing - Jo Triggs In place and ongoing - Jo Triggs
We are currently working off a snapshot of the Register and our access to live Register data is restricted. This will continue until the new Register goes live and we implement new data tools and a reporting database. This may hamper our ability to provide the right data in a timely way when responding to ad-hoc requests.	A reporting version of the Register was captured in December to enable us to do planned reporting such as the trends report, meaning there will be no impact on such standing information provision. For other requests, such as ad hoc FOIs and PQs, we also use this snapshot but there is a risk that we could receive a question about a variable that is not included in the snapshot. This would require assistance from a key staff member in the Register team and may not be possible at short notice. The implementation of these new tools and systems will be prioritised, to ensure that impact and this interim period is minimised. Teams, such as the Inspectorate, have backup plans for the gap between cutover and when the new register feeds into existing systems or processes (inspectors' notebooks, RBAT, QSUM etc.) to ensure relevant data is available.	Register snapshot captured December 2020. Understanding of potential need for cross team support in place and ongoing – Nora Cooke O'Dowd Prioritised as part of Information team delivery – Dan Howard In place - Dan Howard, Sharon Fensome-Rimmer

Causes / sources	Controls	Status / timescale / owner
Until more development is done on reporting from the new Register, we will be unable to update data on Choose a Fertility Clinic. Over time it will stop delivering on its unique selling point, to be a source of independent, timely, accurate information to inform patients' treatment choices.	We updated the data available on CaFC ahead of the Register migration, to ensure that 2019 treatment data can be accessed, bringing this up to date. This will delay CaFC becoming out of date, but does not close the risk. Ongoing controls need to be agreed, but conversations are underway about next steps and approaches we may take, so that we can plan any control activities into business plans for 2021/22 or 2022/23 as needed.	Completed February 2021 – Dan Howard Discussions about future mitigation plans underway – Peter Thompson
There are gaps in key strategic information flows on our website, for instance after treatment, resulting in missed opportunities to share information.	Digital Communications Board with membership from across the organisation in place to discuss information available and identify any gaps and what to do to fill these.	In place and ongoing - Jo Triggs
Given the advent of increased DNA testing, we no longer hold all the keys on donor data (via our Opening the Register (OTR) service). Donors and donor conceived offspring may not have the information they need to deal with this.	Maintain links with donor organisations to mutually signpost information and increase the chance that this will be available to those in this situation. Maintain links with DNA testing organisations to ensure that they provide information to those using direct to consumer tests about the possible implications. Raise this in any review of the Act.	In place and ongoing - Jo Triggs In place and ongoing - Laura Riley Future measure – Peter Thompson
Our OTR workload will increase and change in 2021/2023 (when children born after donor anonymity was lifted begin to turn 16 and 18) and we may lack the capability to deal sensitivity with donor issues.	Plans to undertake service redesign work to review resourcing and other requirements for OTR to ensure these are fit for purpose.	Future control – scoping started in Q4 2020/2021 - Dan Howard
The OTR service may be negatively impacted by an influx of applications following reopening after being paused, with demand outstripping our ability to respond. Note, this is being managed as a live issue as at April 2021.	Our focus is on accuracy and effective support for applicants; therefore, we have temporarily ceased reporting against our usual KPI, during the period of dealing with this pent-up demand. We are continuing to clearly communicate with applicants and the sector to manage expectations. We have recruited additional temporary resource to manage demand.	New starter being trained from April 2021 – Dan Howard
Risk that key regulatory information will be overlooked by stakeholders owing to the number of different communication channels and information sources.	There is a statutory duty for PRs to stay abreast of updates, and we provide key information via Clinic Focus. We duplicate essential communications by also sending via email to the centres' PR and LH (for instance, all Covid-19 correspondence).	In place – Rachel Cutting

Causes / sources	Controls	Status / timescale / owner
	We ensure that the Code and other regulatory tools are up to date, so that clinics find the right guidance on the Portal when they need it regardless of additional communicated updates. We plan to implement a formal annual catch-up between clinics and an inspector. Note: that due to revised inspection approach due to Covid-19 these plans have been delayed.	In place – Laura Riley, Joanne Anton Future control to consider following Covid-19 – Rachel Cutting
We don't provide tangible insights for patients in inspection reports to inform their decision making; because of this, we could be seen as less transparent than other modern regulators.	Review of inspection reports is underway to identify future improvements to inspection reports. Consideration of further changes to the information we publish in discussions on 'regulation and transparency' at Authority meetings. We do provide patient and inspector ratings on CaFC to provide some additional insight into clinics.	Early work underway, but likely to complete late-2021 – Rachel Cutting In place – Rachel Cutting
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
None.		

P1: There is a risk that we don't position ourselves effectively and so cannot influence and regulate optimally for current and future needs.

Inherent risk level:			Residual risk level:		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	4	16	**2**	**3**	**6- Medium**
Tolerance threshold:					**9- Medium**
Status: Below tolerance					

Risk area	Risk owner	Links to which strategic objectives?	Trend
Positioning and influencing P1: strategic reach and influence	Clare Ettinghausen – Director of Strategy and Corporate Affairs	Shaping the future and whole strategy	⇔⇔⇔⇔

Commentary
This risk is about us being in a position to influence effectively to achieve our strategic aims. If we do not ensure we are, we may not be involved in key debates and developments, others will not present the HFEA perspective, meaning we may be voiceless, or our strategic impact may be limited. Discussions occurred with the Authority in January 2021 about our ongoing communications approach, including the 30th anniversary of the HFEA. This supports our thinking on strategic positioning and will ensure that we are best placed to deliver on the Authority's strategic ambitions. The response to the Covid-19 pandemic has required close working with many other organisations and professional bodies, as well as increased engagement with the sector, which has strengthened our strategic positioning and reduced the likelihood of this risk. Consequently, SMT reduced the risk score in March 2021.

Causes / sources	Controls	Status/timescale / owner
We do not currently have all the contacts and reach we need to undertake key work, for instance, with GPs, meaning aspects of the strategy would be too big to complete within our resources.	Ensure a stakeholder engagement plan is agreed and revisited frequently. Note: revised stakeholder plans will need to be agreed with our new Chair from April 2021. Stakeholder identification undertaken for all projects to ensure that these are clear from the outset of planning, and that we can plan communications, involvement and if necessary, consultations, appropriately.	Early work done further discussions with Authority planned– Clare Ettinghausen In place - Paula Robinson

Causes / sources	Controls	Status/timescale / owner
We are unable to persuade partner organisations to utilise their powers/influence/resources to achieve shared aims.	Early engagement with such organisations, to build on shared interests and reduce the likelihood of this becoming an issue. For instance, the treatment add-ons working group.	In place - Clare Ettinghausen
The sector can take a different view on the evidence HFEA provides in relation to Add-ons and so we may be ignored.	The working group for the add-ons project will focus on building on earlier consensus and pull together key stakeholders to reduce the likelihood of guidance and evidence being dismissed. SCAAC sharing evidence it receives and having an open dialogue with the sector on add-ons.	Ongoing - Laura Riley
When there are changes, HFEA and sector interests can be in conflict, damaging our reputation. This may particularly be the case in relation to Covid-19 and the use and removal of General Directions 0014 (GD0014).	Decisions taken within the legal framework of the Act and supported by appropriate evidence, which would ensure these are clear and defensible. Framework for decision making around removing GD0014 drawn up following Authority discussion.	In place - Peter Thompson In place – Rachel Cutting
We lack opportunities to engage with early adopters or initiators of new treatments/innovations or changes in the sector.	Regular engagement with SCAAC enables developments to be flagged for follow up by compliance/policy teams. Routine discussion on innovation and developments at Policy/Compliance meetings to ensure we consider developments in a timely way. Inspectors feed back on new technologies, for instance when attending ESHRE, so that the wider organisation can consider the impact of these. We plan to investigate holding an annual meeting with key innovators (in industry) in the future.	In place - Laura Riley/Joanne Anton In place - Laura Riley/Joanne Anton In place and ongoing – Sharon Fensome-Rimmer Future control, delayed due to Covid-19 but to be reviewed in Q3/4 2021/2022 - Rachel Cutting
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
DHSC: The Department may not consider future HFEA regulatory interests or requirements when planning for any future consideration of relevant legislation which could compromise the future regulatory regime.	Early engagement with the Department to ensure that they are aware of HFEA position in relation to any future review of the legislation. Provided a considered response to the Department's storage consent consultation to give the HFEA position.	Ongoing - Peter Thompson Completed - Joanne Anton

Causes / sources	Controls	Status/timescale / owner
Government: Any consideration of the future legislative landscape may become politicised.	There are no preventative controls for this, however, clear and balanced messaging between us, the department and ministers may reduce the impact. Develop improved relationships with MPs and Peers to ensure our views and expertise are taken into account.	Ongoing - Peter Thompson
Government: Consideration of changes to the regulatory framework may be affected by political turbulence (for instance changes of Minister).	There are no preventative controls for this, however, we will ensure that we are prepared to effectively brief any future incumbents to reduce turbulence. We would also do any horizon scanning as the political landscape changed if needed.	Ongoing - Peter Thompson

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

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

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
Covid-19 and the implementation of GD0014 caused reduced treatment activity during 2020-2021 meaning this risk became a live issue, although we were given assurance of cover by the Department. Close monitoring of treatments and fee income throughout January – March 2021, and projections for the current 2021-2022 financial year, suggest that the risk related to reduced fee income is smaller for the year ahead and we would be able to support ourselves from reserves if fees were below our projections. We have also had confirmation of our budget from the Department of Health and Social Care, which provides greater certainty. SMT agreed that this did not make a fundamental difference to the score as at June 2021. An initial options appraisal for a fee review project was agreed with Authority in June 2020. A consultation and modelling for the new income model will follow but owing to the impact of Covid-19 there is now some uncertainty around the timing of this work. Discussions are ongoing with the Department. This review, when it occurs, should ensure that the income model is fit for purpose and reflects the changing nature of sector activity, and set the HFEA up for the future.

Causes / sources	**Controls**	**Timescale / owner**
There is uncertainty about the annual recovery of treatment fee income – this may not cover our annual spending. This is a live issue as we have reduced income for as long as GD0014 (version 2) is in place, however it is a smaller risk than at the height of the pandemic. Although clinics have reopened it will take some time for activity to return to 'normal' levels.	Heads see quarterly finance figures and would consider what work to deprioritise or reduce should income fall below projected expenditure. We would discuss with the Authority if key strategic work needed to be delayed or changed. 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.	CMG monthly and Authority when required – Peter Thompson Paused due to impact of pandemic on fee income and activity levels Planning underway – Peter

Causes / sources	Controls	Timescale / owner
	We plan to undertake a fee review project (timing TBC) to ensure that the income model is fit for purpose and reflects the changing nature of sector activity. We are discussing with the Authority and Department of Health and Social Care how this will be taken forward	Thompson and 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. As at April 2021 we had reduced income due to the deployment of GD0014 in response to Covid-19 and the subsequent reopening of the sector.	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 October 2020. 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.	Given the Covid-19 related drop in income, we have actively employed this control – Richard Sydee Control under quarterly review as sector reopens – 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
Additional funds have been required for the completion of the data migration work and this will constrain HFEA finances and may affect other planned and ad hoc work. Note: PRISM delivery has now been delayed further into 2021/2022 which will have a financial impact.	The most cost-effective approach was taken to procure external support to reduce costs and the resulting impact. Ongoing monitoring and reporting against control totals to ensure we do not overspend. Funding was received from the Department to complete the PRISM programme. Careful consideration of ongoing cost implications of PRISM delays for 2021/2022 and discussion of approach and risk management with AGC. Additional financial cover was agreed with the Department in 2021-2022 to help cover the costs of extended delivery.	In place – Richard Sydee Ongoing, – Richard Sydee Ongoing – Richard Sydee
The Stratford office may cost more than the current office, once all facilities and shared elements are considered, leading to opportunity costs.	Costs for Redman Place (the Stratford building) will be allocated on a usage basis which will ensure that we do not pay for more than we need or use. The longer, ten-year lease at Redman Place will provide greater financial stability, allowing us to forecast costs over a longer period and adjust other expenditure, and if necessary, fees,	Ongoing but we await confirmation of overarching procurement arrangements from central

Causes / sources	Controls	Timescale / owner
The Finance and procurement strand of the project has been delayed; we await final estimates of the cost to HFEA, though have been assured that calculations have been completed. Note: As at April 2021, although this is not yet finalised, it looks likely that the new office will be cheaper. Costs are being mapped for the next financial year.	accordingly, to ensure that our work and running costs are effectively financed. The accommodation at Redman Place should allow us to reduce some other costs, such as the use of external meeting rooms, as we will have access to larger internal conference space not available at Spring Gardens. All provided cost estimates to date suggest a material reduction in the operating costs of Redman Place when compared to Spring Gardens.	programme - Richard Sydee We await a final MOTO from DHSC which is anticipated in May 2021
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 member 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) – Samuel Akinwonmi
Failure to comply with Treasury and DHSC spending controls and finance policies and guidance may lead 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 (ALBs / DHSC)	**Control arrangements**	**Owner**
DHSC: Covid-19 impacts on HFEA income.	The final contingency for all our financial risks is to seek additional cash and/or funding from the DHSC and we are in ongoing discussions with the Department about this issue for the 2021/2022 business year having received confirmation from them for cover in 2020/2021.	Ongoing - Richard Sydee

Causes / sources	Controls	Timescale / owner
DHSC: Legal costs materially exceed annual budget because of unforeseen litigation.	Use of reserves, up to appropriate contingency level available at this point in the financial year. 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. Annual budget has been agreed with DHSC Finance team. GIA funding has been agreed through to 2021.	Quarterly accountability meetings (on-going) – Richard Sydee 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**
5	4	20 – Very high	**3**	**3**	**9 - Medium**
Tolerance threshold:					**12 - High**
Status: Below tolerance.					

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

Commentary
This risk and the controls are focused on organisational capability, rather than capacity, though there are obviously some linkages between capability and capacity. As at June 2021, turnover is starting to increase, which puts strain on staff generally while covering gaps, inducting new starters and managing knowledge gaps. In recent months, recruitment has been successfully undertaken throughout the Covid-19 pandemic, with effective remote onboarding of new starters. If churn reaches a level of 15-20%, this would become an issue, rather than merely a risk, and we would need to review our controls, and possibly reprioritise certain pieces of work. This would depend on the scenario and the posts affected by churn. AGC receive 6-monthly updates on capability risks to consider our ongoing strategies for the handling of these, to allow them to track progress. Looking further ahead, we need to find ways to tackle the issue of development opportunities, to prevent this risk increasing. 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. Unfortunately, this work has not progressed further due to Covid-19, although conversations about such development opportunities continue on an individual level. Management of Board and senior executive capability is captured in the separate C2 risk, below.

Causes / sources	**Mitigations**	**Status/Timescale / owner**
High turnover, sick leave etc., leading to temporary knowledge loss and capability gaps. Note: this is a more acute risk for our smaller teams.	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

Causes / sources	Mitigations	Status/Timescale / owner
	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. Contingency: In the event of knowledge gaps, we would consider alternative resources such as using agency staff, or support from other organisations, if appropriate.	In place – Yvonne Akinmodun and relevant managers In place – Peter Thompson In place – Relevant Director alongside managers
Poor morale leading to staff leaving, opening up capability gaps.	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 staff intranet enables regular internal communications. Ongoing CMG discussions about wider staff engagement (including surveys) to enable management responses where there are areas of concern. Policies and benefits are in place that support staff to balance work and life (stress management resources, mental health first aiders, PerkBox) promoting staff to feel positive about the wider package offered by the HFEA. This may boost good morale.	In place, ongoing – Peter Thompson In place – Jo Triggs In place, staff survey undertaken June 2020 – Yvonne Akinmodun In place and review planned in 2021 - Peter Thompson
Work unexpectedly arises or increases for which we do not have relevant capabilities.	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. 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. Oversight of projects by both the monthly Programme Board and CMG meetings. Review of project guidance to support early identification of interdependencies and products in projects, to allow for effective planning of resources.	In place – Paula Robinson In place – Paula Robinson In place – Paula Robinson Ongoing review in progress 2021-2022– Paula Robinson

Causes / sources	Mitigations	Status/Timescale / owner
	Planning and prioritising data submission project delivery, within our limited resources. Skills matrix being circulated for completion by teams in 2021/2022 to enable better oversight of organisational skills mix and deployment of resource.	In place until project ends – Dan Howard In progress – Yvonne Akinmodun
Not putting actions in place to realise the capability benefits of colocation with other organisations, arising out of the office move, such as the ability to create career pathways and closer working.	Active engagement with other organisations early on and ongoing. We are collaborating with other relevant regulators to see what more can be done to create career paths and achieve other benefits of working more closely, including a mentorship programme. **Note**: delayed due to Covid-19 impacts.	Early progress, ongoing – Yvonne Akinmodun
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
Government/DHSC The UK leaving the EU may have ongoing consequences for the HFEA which we would have to manage	Since December 2018, we have run an EU exit project to ensure that we have fully considered implications and are able to build enough knowledge and capability to handle the effects of the UK's exit from the EU. We have progressed this project through the transition period and now beyond. We continue to engage with clinics on the impacts. Authority and AGC are updated at their meetings, as appropriate. We continue to work closely across the HFEA and with the DHSC to ensure we are prepared for any further consequences of the UK leaving the EU. This includes implementing the Northern Ireland Protocol as it applies to HFEA activity across the UK.	Communications ongoing – Clare Ettinghausen/Andy Leonard
In-common risk Covid-19 (Coronavirus) may lead to high levels of staff absence leading to capability gaps or a need to redeploy staff.	Management discussion of situation as it emerges, to ensure a responsive approach to any developments. We have reviewed our business continuity plan to ensure it is fit for purpose.	Ongoing with Business continuity plan reviewed at CMG in April 2021- Peter Thompson

C2: Loss of senior leadership (whether at Board or Management level) leads to a loss of knowledge and capability which may impact formal decision-making and strategic delivery.

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	4	16- High	**3**	**4**	**12 - High**
Tolerance threshold:					**4 - Low**
Status: **Above tolerance**					

Risk area	Risk owner	Links to which strategic objectives?	Trend
Estates C2: Board capability	Peter Thompson Chief Executive	Whole strategy.	⇔⇧⇔⇔

Commentary
In April 2021, the Chief Executive and Risk and Business Planning Manager reframed this risk following discussion with AGC, SMT and the Chair. This risk has been amended to now reflect both the risks related to both Board and senior executive leadership. Although the causes and impacts are different, many of the mitigations are similar, and both would have an impact on the organisation's external engagement and potentially strategic delivery. The HFEA board is unusual as members undertake quasi-judicial decision-making as part of their roles, sitting on licensing and other committees. This means that changes in Board capability and capacity may impact the legal functions of the Authority. We need to maintain sufficient members with sufficient experience to take what can be highly controversial decisions in a robust manner. As such our tolerance threshold for this risk is low. The score of this risk was reduced in March 2021 to reflect the positive effect of appointments made and the extension of key members' terms until the end of the year which provides some continuity. However, we have reviewed the overall risk score in the light of two recent developments. First, three members' first terms are due to end over summer 2021 and failure to reappoint could pose particular risks in key committees. Second, the inclusion of senior executive risks. Taken together, we have since raised the overall risk. We are actively discussing controls, for instance we are in discussion with the DHSC about the reappointment of the three members and the recruitment campaign that will be needed to replace the further five members at the end of the year. Board capability has been a key early discussion with our new Chair and proposals are with the DHSC to manage upcoming membership terms.

Causes / sources	Mitigations	Status/timescale / owner
A precipitous reduction in available members (due to member terms ending) would put at risk our ability to meet our statutory responsibilities to licence fertility clinics and	Membership of licensing committees has been actively managed to ensure that formal decision-making can continue unimpeded by the recent board vacancies. However, there is no guarantee that this would be possible for future vacancies, especially if there were several at once and	In place, ongoing - Paula Robinson

Causes / sources	Mitigations	Status/timescale / owner
research centres and authorise treatment for serious inherited illnesses.	bearing in mind that a lay/professional balance must be maintained for some committees. This is being actively discussed for upcoming possible vacancies.	
The loss of a member of the senior leadership team (for instance through retirement, leaving the organisation for a new role etc) creates a leadership/knowledge gap.	Note: We cannot mitigate the cause of this risk, since staff may choose to leave the organisation for personal reasons. However, we can mitigate the consequences. Responsibilities could be shared across SMT and Heads to cover any gaps and maintain leadership, decision-making and oversight (this would include Chairing ELP which may be delegated under Standing Orders). Good induction process to ensure that new staff are onboarded efficiently. Effective use of delegation, to build capability of less senior staff, to enable them to step up in the case of senior staff absences (either temporarily or to apply for the role permanently in the case of staff leaving). Chief Executive would discuss recommendations for cover with the Chair if he were to move on from the organisation, to ensure that responsibilities were covered during any gap before appointment. Other controls (handover, knowledge capture, processes etc) per the wider staff turnover risk above. More explicit succession planning is being considered but must be balanced with a free and fair recruitment process. Clear, documented plans to enable more straightforward management of such a situation when it occurs.	In place – Peter Thompson In place - Yvonne Akinmodun with relevant Manager for specific role In place – Relevant Director alongside managers As required – Director and staff as relevant As required – Peter Thompson, Julia Chain Future control – in discussion – Peter Thompson Future control – in discussion – Peter Thompson
Any member recruitment often takes some time and therefore give rise to further vacancies and capability gaps. The recruitment process is run by DHSC meaning we have limited power to influence this risk source.	In January 2021, recruitment was successful for four Board posts. We are now focussing on streamlining induction to ensure that Members are brought up to speed as quickly as practicable (see risks below). This risk cause remains for future recruitment and we remain in discussion on the ongoing management of this.	Underway- Peter Thompson

Causes / sources	Mitigations	Status/timescale / owner
Historically, decisions on appointments have taken some time which may create additional challenges for planning (the annual report from the commission for public appointments suggests appointments take on average five months).		
Recruitment to SMT or Head post often takes some time which could create a leadership gap.	Heads could temporarily act up into Director roles to manage any pre-recruitment gaps. The same would be true of manager level staff acting up for Heads.	In place, discussed as required – relevant Manager with Yvonne Akinmodun
Several current Board members are on their second terms in office, which expire within the same period (from summer 2021).	We are discussing options with the Department for managing the cycle of appointments, in order to reduce the ongoing impact of this. The targeted extension of some members extends the proximity of this issue somewhat.	In progress, ongoing - Peter Thompson
The induction time of new members (including bespoke legal training) can be significant, particularly for those sitting on licensing committees, may lead to a loss of collective knowledge and potentially an impact on the quality of decision-making. Evidence from current members suggests that it can take up to a year for members to feel fully confident.	The Governance team has reviewed recruitment information and member induction to ensure that this is as smooth as possible. Targeted extensions, noted above, should bridge this period of learning and therefore support new members.	In place and ongoing - Paula Robinson
Induction of new members to licensing and other committees, will require a significant amount of internal staff resource and could reduce the ability of the governance and other teams to support effective decision-making.	We have been mindful of this resource requirement when planning other work, in order to limit the impact of induction on other priorities.	In progress, - Peter Thompson, Paula Robinson
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Status/timescale / owner**
Government/DHSC The Department is responsible for our Board recruitment but is	Clear communication with the Department about the management of this risk and mitigations that sit outside of HFEA control.	Ongoing - Peter Thompson

Causes / sources	Mitigations	Status/times cale / owner
bound by Cabinet Office guidelines.		
Government/DHSC DHSC is responsible for having an effective arm's length body in place to regulate ART. If it does not ensure this by effectively managing HFEA Board recruitment, it will be breaching its own legal responsibilities.	Clear communication with the Department about the management of this risk and mitigations that sit outside of HFEA control.	Ongoing - Peter Thompson
Government/DHSC HFEA operates in a sensitive area of public policy, meaning there may be interest from central government in the appointments process. This may impact any planned approach and risk mitigations and give rise to further risk.	Clear communication with the Department about the management of this risk and mitigations that sit outside of HFEA control.	Ongoing - Peter Thompson

CS1: There is a risk that the HFEA is subject to a cyber-attack, resulting in data or sensitive information being compromised, or IT services being unavailable.

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**
Status: At tolerance					

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

Commentary

Cyber-attacks and threats are inherently very likely. Our approach to handling these risks effectively includes ensuring we:

- have an accurate awareness of our exposure to cyber risk
- have the right capability and resource to handle it
- undertake independent review and testing
- are effectively prepared for a cyber security incident
- have external connections in place to learn from others.

We continue to assess and review the level of national cyber security risk and act as necessary to ensure our security controls are robust and are working effectively.

Delays to PRISM delivery necessitate the continued use of EDI in clinics. Many clinics use older server technology to run our EDI gateway within their clinic or organisation resulting in an increased cyber risk while that technology is in use. Many have upgraded their infrastructure to reduce the likelihood of a cyber incident. The related cyber risk concerns an attack on the clinic's infrastructure – all have local logical and physical security controls in place. All submission data via EDI is encrypted in transit. We continue to work with clinics to support the upgrade of their server infrastructure.

Causes / sources	Controls	Timescale / owner
Insufficient board oversight of cyber security risks, resulting in them not being managed effectively.	Routine cyber risk management delegated from Authority to Audit and Governance Committee which receives reports at each meeting on cyber-security and associated internal audit reports to assure the Authority that the internal approach is appropriate and ensure they are aware of the organisation's exposure to cyber risk. The Deputy Chair of the Authority and AGC is the cyber lead who is regularly appraised on actual	In place – Dan Howard In place - Peter Thompson

Causes / sources	Controls	Timescale / owner
	and perceived cyber risks. These would be discussed with the wider board if necessary. Annual cyber security training in place to ensure that Authority are appropriately aware of cyber risks and responsibilities.	Last undertaken January 2020. We are continuing to investigate cyber security courses to identify the most appropriate one for Authority members. – Dan Howard
Insufficient executive oversight of cyber security risks, resulting in them not being managed effectively	Cyber security training in place to ensure that all staff are appropriately aware of cyber risks and responsibilities. Regular review of cyber / network security policies to ensure they are appropriate and in line with other guidance. We undertake independent review and test our cyber controls, to assure us that these are appropriate. Regular review of business continuity plan to ensure that this is fit for purpose for appropriate handling cyber security incidents to minimise their impact. Additional online Business Continuity training for Business Continuity Group.	Undertaken by staff October/November 2020 – Dan Howard Update agreed at CMG in June 2020– Dan Howard In place, review occurred January 2021 – Dan Howard In place, CMG considered this in April 2021 – Dan Howard In place and being completed – Dan Howard
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.	Penetration testing of newly developed systems (PRISM, the Register) assure us that development has appropriately considered cyber security. Clear information security guidance to HFEA staff about how identifying information should be shared, especially by the Register team, to reduce the chance of this being vulnerable.	Testing is undertaken regularly, last completed in January 2021 – Dan Howard In place – Dan Howard

Causes / sources	Controls	Timescale / owner
The IT support function is small so may not provide us with the cyber security resource that we need (ie, emergency support in the case of dealing with attacks)	We have an arrangement with a third-party IT supplier who would be able to assist if we did not have enough internal resource to handle an emergency for any reason.	Contract in place until June 2021. We expect to take the option to extend this until June 2023 – Dan Howard
We cannot mitigate effectively for emerging or developing cyber security threats if we are not aware of these.	We maintain external linkages with other organisations to learn from others in relation to cyber risk.	Ongoing (such as ALB CIO network and Cyber Associates Network) – Dan Howard
Technical or system weaknesses could lead to loss of, or inability to access, sensitive data, including the Register.	We undertake regular penetration testing to identify weaknesses so that we can address these. We have advanced threat protection in place to identify and effectively handle threats. Our third-party IT supplier undertakes daily checks on our server infrastructure to monitor for any errors and to monitor for any security issues or increased threats. We regularly review and if necessary, upgrade software to improve security controls for network and data access, such as Remote Access Service (RAS) software. We regularly review and if necessary, upgrade software to improve security controls for telephony. We are also currently reviewing whether to redevelop our centres database, Epicentre, in the coming year, since some elements of it are old and out of support.	Ongoing, last test took place in January 2021 – Dan Howard In place – Dan Howard In place – Dan Howard Ongoing (Upgrade to Pulse RAS system completed during 2020) – Dan Howard Ongoing (Upgrade to Microsoft Teams system completed 2020) – Dan Howard
Physical devices used by staff are lost, stolen or otherwise fall into malicious hands, increasing chance of a cyber-attack.	Hardware is encrypted, which would prevent access to data if devices were misplaced. Staff reminded during IT induction about the need to fully shut down devices while outside of secure locations (such as travelling) in order to implement encryption	Ongoing (regular reminders sent to staff with security best practice) – Dan Howard

Causes / sources	Controls	Timescale / owner
Remote access connections and hosting via the cloud may create greater opportunity for cyber threats by hostile parties.	All cloud systems in use have appropriate security controls, terms and conditions and certifications (ISO and GCloud) in place. We have an effective permission matrix and password policy. Our web configuration limits the service to 20 requests at any one time. The new Register will be under the tightest security when this is migrated to the cloud.	In place – Dan Howard In place – Dan Howard In place – Dan Howard To be implemented – Dan Howard
The continued use of EDI by clinics during the extended delivery of PRISM means the end-of-life server version used for the EDI gateway application (which processes data from EDI or 3rd party servers into the HFEA Register) continues to be used. This may therefore be more vulnerable to attack as it becomes unsupported.	Data submitted through the EDI gateway application is encrypted in transit, which reduces the likelihood of sensitive information being accessed.	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.		

OM1: There is a risk that the HFEA fails to capitalise on or respond effectively to changes affecting the organisation and its ways of working (including related to office working and Covid-19) hampering strategic and statutory delivery.

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

Risk area	Risk owner	Links to which strategic objectives?	Trend
Operating Model OM1: Management of changes to HFEA operating model	Peter Thompson Chief Executive	Whole strategy.	⇔⇔⇔⇔

Commentary
In November 2020 SMT agreed to reframe the remaining risks from the previous E1 estates/office move risk, once the physical move had occurred, and instead pick these up with a new ways of working/change risk. SMT discussed this new risk in January 2021, drawing various key causes of ongoing change to the HFEA operating model into a single risk. This risk will be reviewed carefully over the coming months to ensure that it fully reflects emergent risks, and appropriate granularity, including reflecting risks arising from new ways of working brought in by PRISM once it launches. SMT reflected in March 2021 that the very active consideration of controls, engagement with staff and baseline high level of flexibility offered by the organisation meant they felt the residual risk was lower. Looking ahead, a key aspect of managing this risk will be being alert to what other organisations are doing; maintaining our relative flexibility while meeting our organisational needs is likely to be a way of attracting and retaining staff ongoing.

Causes / sources	Controls	Status/Timescale / owner
The facilities provided in the Stratford office may not fulfil all HFEA requirements and desired benefits, such as ability to host key corporate meetings. Note: Covid-19 may have altered the requirements of the HFEA and we have not yet returned to office based working, meaning that although the move has competed this risk remains.	HFEA requirements were specified up front and feedback given on all proposed designs. Outline plans were in line with HFEA needs and we had staff on the working groups set up to define the detail. Our requirements and ways of working are being revisited in the light of the changed circumstances we are in due to Covid-19. AV equipment is not yet fully installed as at June 2021. If lower-priority requirements are unable to be fulfilled, conversations will take place about	Ongoing – Richard Sydee Ongoing as part of Covid-19 management – Richard Sydee Contingency if required –

Causes / sources	Controls	Status/Timescale / owner
	alternative arrangements to ensure HFEA delivery is not adversely affected.	Richard Sydee
Stratford is a less desirable location for some current staff due to: • increased commuting costs • increased commuting times • preference of staff to continue to work in central London for other reasons, leading to lower morale and lower levels of staff retention as staff choose to leave following the move.	We will review the excess fares policy to define the length of time and mechanism to compensate those who will be paying more following the move to Stratford. Efforts taken to understand the impact on individual staff and discuss their concerns with them via staff survey, 1:1s with managers and all staff meetings to inform controls. These have informed the policies developed. Conversely, there will be improvements to the commuting times and costs of some staff, which may improve morale for them and balance the overall effect.	Begun but to be completed (this is now subject to Covid-19 developments) – Yvonne Akinmodun, Richard Sydee Done - Yvonne Akinmodun,
There is a risk that staff views on the positives and negatives of homeworking due to Covid-19 are not taken into account, meaning we miss opportunities for factor these into planning our future operating model and alienate staff by not considering their views, for instance on flexible working.	Heads discuss impacts with teams on a regular basis and feed views into discussions at CMG. Regular communication to staff about the developing conversation and direction of travel through all staff meetings and the intranet. A further survey of staff is being planned, to inform any policy reviews.	Ongoing with survey prior to return to the office – Peter Thompson
The need to operate with revised arrangements during Covid-19 and social distancing may delay consideration of our ongoing post-covid operating model, leading to staff seeing management as extending uncertainty about arrangements, inconsistent application of temporary arrangements and inequity, causing lower morale and levels of staff retention.	Clarity provided to staff that current arrangements for working from home will continue until at least end June 2021. CMG to balance staff desire for certainty about post-Covid-19 arrangements with need for flexibility of response during a period of ongoing change. CMG to discuss likely policies that will be applicable following social-distancing arrangements to provide assurance, for instance about maximum office attendance requirements.	Discussions in progress – Peter Thompson
Current staff may not yet feel informed about the facilities in the new office, leading to anxiety and lower morale.	Conversations about ways of working occurred throughout the office move project, to ensure that the project team and HFEA staff were an active part of the discussions and development of relevant policies and have a chance to raise questions.	Ongoing – Richard Sydee

Causes / sources	Controls	Status/Timescale / owner
	An open approach was taken to ensure that information was cascaded effectively during the project. We have a separate area on the intranet and Q&A functionality where all information is shared. Staff have had opportunities to visit the site so that they feel prepared. Staff engagement group was in place to ensure wide engagement as we approached the move. Management of ongoing ways of working tasks and engagement with staff being done through CMG as part of HFEA move project closure and post-project oversight. As the situation relating to the pandemic evolves, we are seeking clarity on the availability of facilities, so that this can be communicated to staff.	
The move to a new office and Covid-19 arrangements will lead to ways of working changes we may be unprepared for.	CMG has been discussing ways of working in the aftermath of Covid-19 and in relation the office move, to ensure that these changes happen by design rather than by default. Policies related to ways of working have been agreed and circulated significantly before the move, to ensure that there is time for these to bed in and be accepted ahead of the physical move. Staff have and will continue to be been involved and updated as appropriate.	Discussions each month at CMG until we move back to the office – Richard Sydee Done and to continue as these are reviewed in light of Covid-19 - Richard Sydee, Yvonne Akinmodun
There is still uncertainty about arrangements around meetings in Redman Place including: • availability of physical meeting spaces • implications of any ongoing social distancing • AV/VC arrangements and readiness for use • shared desk arrangements • booking procedures and systems If these are not managed effectively or do not work well	Throughout Covid-19 remote working, the organisation has effectively run meetings remotely and could continue to do so for as long as is necessary, to ensure that required meetings can continue. Ongoing FM group in place for Redman Place, to coordinate and communicate about arrangements and ensure that these run smoothly.	Ongoing – Peter Thompson In place following central programme closure – Richard Sydee

Causes / sources	Controls	Status/Timescale / owner
this will lead to disruption to core business.		
There are different cultures and working practices in the organisations moving, so there may be perceived inequity about the policy changes made.	During the Redman Place Programme, a formal working group was in place including all the organisations who are moving to Stratford with us, to ensure that messaging around ways of working has been consistent across organisations, while reflecting the individual cultures and requirements of these. We will communicate about any differences, so that staff understand any differences in practice and that the intention is not to homogenise practices. Ongoing working groups in place following programme closure in March 2021.	Ways of working group work completed, follow on communic-ations being coordinated across all organisations – Richard Sydee
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
NICE/CQC/HRA/HTA – IT, facilities, ways of working interdependencies.	Ongoing building working groups with relevant IT and other staff such as HR. Informal relationship management with other organisations' leads.	In place – Richard Sydee, DHSC

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	**3**	**4**	**12 - High**
Tolerance threshold:					**12 - High**
Status: **At tolerance**					

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

We accept that in a controversial area of public policy, the HFEA and its decision-making will be legally challenged. Our Act and related regulations are complex, and aspects are open to interpretation, sometimes leading to challenge. There are four fundamental sources of legal risk to the HFEA, it may be due to:

- execution of compliance and licensing functions (decision making)
- the legal framework itself as new technologies and science emerge
- policymaking approach/decisions
- individual cases and the implementation of the law (often driven by the impact of the clinic actions on patients).

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 and at their most impactful they could undermine the statutory scheme the HFEA is tasked with upholding. 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.

We have recently been served with a Judicial Review. The risk has therefore materialised.

Causes / sources	Mitigations	Timescale / owner
Legal challenge about the way we have executed our core regulatory functions of inspection and licensing. For instance, clinics challenging	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.	In place – Peter Thompson

Causes / sources	Mitigations	Timescale / owner
decisions taken about their licence.		
Legal challenge if new science, technology or wider societal changes emerge that are not covered by the existing regulatory framework.	Scientific and Clinical Advances Advisory Committee (SCAAC) horizon scanning processes. This provides the organisation with foresight and may provide more time and ability to prepare our response to developments. Case by case decisions on the strategic handling of contentious or new issues in order to reduce the risk of challenge or, in the event of challenge, to put the HFEA in the strongest legal position.	SCAAC horizon scanning meetings annually. In place – Catherine Drennan and Peter Thompson
Legal challenge to policies when others see these as a threat or ill-founded. 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.	Evidence-based and transparent policymaking, with risks considered whenever a new approach or policy is being developed. 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 and implemented related policy and respond effectively to challenge. Business impact target assessments carried out whenever a regulatory change is likely to have a significant cost consequence for clinics meaning that consideration of impacts and how these will be managed is taken into account as part of the policymaking process. Stakeholder involvement and communications in place during policymaking process (for instance via regular stakeholder meetings) to ensure that clinics and others 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 – Laura Riley/Joanne Anton with appropriate input from Catherine Drennan Ongoing - Laura Riley, Joanne Anton In place – Richard Sydee Ongoing - Laura Riley, Joanne Anton
Legal challenges related to clinical implementation of regulation in terms of individual cases (ie, consent-related cases). Ongoing legal parenthood and storage consent failings in clinics and related cases are specific examples. The case-	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. Through constructive and proactive engagement with third parties, the in-house legal function serves to anticipate issues of this sort and prevent challenges. This strengthens our ability to find solutions that do not require legal action.	Ongoing – Catherine Drennan In place – Catherine Drennan

Causes / sources	Mitigations	Timescale / owner
by-case nature of the Courts' approach to matters means resource demands are unpredictable when these arise.	Legal panel in place, as above, enabling us to outsource some elements of the work. 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. We took advice from a leading barrister on the possible options for handling storage consent cases to ensure we take the best approach when cases arise. We also get ongoing ad hoc advice as matters arise. Some amendments were made to guidance in the Code of Practice dealing with consent to storage and extension of storage, this was launched in January 2019. This guidance will go some way to supporting clinics to be clearer about the legal requirements. Additional amendments will be made in the next update. Storage consent has been covered in the revision of the PR entry Programme (PREP).	In place – Peter Thompson Done in 2018/19 and as needed – Catherine Drennan Revised guidance will be provided where appropriate to clinics in 2021– Catherine Drennan PREP launched January 2020 – Catherine Drennan/ Laura Riley, Joanne Anton
Committee decisions or our decision-making processes being contested. ie, Licensing appeals and/or Judicial Reviews. Challenge of compliance and licensing decisions is a core part of the regulatory framework and we expect these challenges even if decisions are entirely well founded and supported. Controls therefore include measures to ensure consistency and avoid process failings, so we are in the best position for when we are challenged, therefore reducing the impact of such challenges.	Compliance and Enforcement policy and related procedures to ensure that the Compliance team acts consistently according to agreed processes. Well-evidenced recommendations in inspection reports mean that licensing decisions are adequately supported and defensible. The Compliance team monitors the number and complexity of management reviews and stay in close communication with the Head of Legal to ensure that it is clear if legal involvement is required, to allow for appropriate involvement and effective planning of work. This process has been clarified in the revised Compliance and Enforcement Policy. Panel of legal advisors in place to advise committees on questions of law and to help	In place but a revised version of the policy to be launched in June 2021– Rachel Cutting, Catherine Drennan In place – Sharon Fensome-Rimmer In place – Sharon Fensome-Rimmer In place – Peter Thompson

Causes / sources	Mitigations	Timescale / owner
	achieve consistency of decision-making processes. Measures in place to ensure consistency of advice between the legal advisors from different firms. Including: • Provision of previous committee papers and minutes to the advisor for the following meeting • Annual workshop • Regular email updates to panel to keep them abreast of any changes. Consistent and well taken decisions at licence committees supported by effective tools for committees and licensing team (licensing pack, Standard operating procedures, decision trees etc) which are regularly reviewed.	Since Spring 2018 and ongoing – Catherine Drennan In place – Paula Robinson
Any of the key legal risks escalating into high-profile legal challenges resulting in significant resource diversion and reputational consequences for the HFEA which risk undermining the robustness of the regulatory regime.	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. We have sought to build constructive relationships with legal representatives who practice in the sector and the tone of engagement with them means that challenge is more likely to be focused on matters of law than on the HFEA. Internal mechanisms (such as the Corporate Management Group, CMG) in place to reprioritise workload should this become necessary.	In place – Catherine Drennan, Joanne Triggs In place – Peter Thompson, Catherine Drennan In place – Peter Thompson
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
DHSC: If HFEA face unexpected high legal costs or damages which it could not fund. This is an interdependent risk as the Department must ensure the ability to maintain the regulatory regime.	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: We rely upon the Department for any legislative changes in response to legal risks or impacts.	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	In place – Peter Thompson

Causes / sources	Mitigations	Timescale / owner
	necessary, this would include agreeing any associated implementation budget. Departmental/ministerial sign-off for key documents such as the Code of Practice in place.	
DHSC: The Department may be a co-defendant for handling legal risk when cases arise.	We work closely with colleagues at the Department to ensure that the approach of all parties is clear and is coordinated wherever possible. We also pre-emptively engage on emerging legal issues before these become formal legal matters.	In place – Peter Thompson

CV1: There is a risk that we are unable to undertake our statutory functions and strategic delivery because of the impact of the Covid-19 Coronavirus.

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	4	16 – High	**2**	**3**	**6- Medium**
Tolerance threshold:					**12- High**
Status: **Below tolerance**					

Risk area	**Risk owner**	**Links to which strategic objectives?**	**Trend**
Business Continuity CV1: Coronavirus	Peter Thompson Chief Executive	Whole strategy.	⇔⇔⇔⇔

Commentary
Risk management of these risk causes has been our organisational priority since the beginning of the pandemic. All staff are working from home and a strategy to manage inspections is in place. Communications to the sector and patients are in place and ongoing. A business continuity group meets regularly to consider risks and ensure an effective response is developed and maintained. Our revised inspection processes are effective and include comprehensive risk assessment and controls; we are assured that we can effectively maintain this regulatory function. Licensing has continued effectively remotely. SMT considered the risk score in March and decided that the effective inspection methodology reduced the impact of this risk, as the controls ensured we are able to continue to undertake this statutory function, bringing the score down. The implementation of the methodology has caused a secondary risk, while it beds in, but that is being managed and is captured under RF1.

Causes / sources	**Controls**	**Status/Timescale / owner**
Risk of providing incorrect, inconsistent or non-responsive advice to clinics or patients as guidance and circumstances change (ie, not updating our information in a timely manner) and this leading to criticism and undermining our authoritative position as regulator.	Business continuity group (including SMT, Communications, HR and IT) meeting frequently to discuss changes or circumstances and planning timely responses to these. Out of hours media monitoring being undertaken, to ensure that we respond to anything occurring at weekends or evenings in a timely manner. Close communication with key sector professional organisations to ensure we are ready to react to any developments led by them (such as guidance updates). Proactive handling of clinic enquiries and close communication with them.	In place, ongoing – Richard Sydee In place - SMT and communications team In place and ongoing – Clare Ettinghausen In place and ongoing – Sharon

Causes / sources	Controls	Status/Timescale / owner
	Careful monitoring of the need to update information and proactive handling of updates. Public enquiries about Coronavirus are being triaged, with tailored responses in place. Enquirers are being directed to information on our website, to ensure that there is a single source of truth and this is up to date. Enquiries team have additional support from Managers and Directors. We have reviewed our approach regularly to ensure that this is fit for purpose. Close monitoring of media (including social) to identify and respond to any perceived criticism to ensure our position is clear. Regular review of communications activities to ensure they are relevant and effective.	Fensome-Rimmer, Rachel Cutting Joanne Triggs – in place In place and under regular review – Laura Riley In place – Jo Triggs
Risk of being challenged publicly or legally about the HFEA response, resulting in reputational damage or legal challenge. (This risk also therefore relates directly to LC1 above)	As above – ensuring approach is appropriate. As above – continuing to liaise with professional bodies. We may choose to put out a press release in case of public challenge. Legal advice has been sought to ensure that HFEA actions are in line with legislative powers. Further advice available for future decisions. Ability to further engage legal advisors from our established panel if we are challenged.	In place – Richard Sydee Ongoing - Rachel Cutting If required - Joanne Triggs Done – Peter Thompson If required – Peter Thompson, Catherine Drennan
Gaps in HFEA staffing due to sickness, caring responsibilities etc	Possible capability gaps have been reviewed by teams to ensure that these are identified and managed. Other mitigations as described under the C1 risk.	In place – Yvonne Akinmodun
Risk of disproportionate impact of coronavirus on staff from black and ethnic minority backgrounds. Note: we do not have evidence of this being an issue within the HFEA.	Decision taken to delay routine return to the office subject to government guidance, reducing work-related risk. We are engaging with other similar organisations to consider possible approaches to managing this risk. We have considered the impact as part of planning for the return to inspections and office working, including individual risk assessments for inspection staff, performed before each inspection.	In progress – Yvonne Akinmodun In place – Sharon Fensome-Rimmer

Causes / sources	Controls	Status/Timescale / owner
Clinics stop activity during the epidemic and so we are unable to inspect them within the necessary statutory timeframes.	Extending of licences (noted above) should remove this risk by ensuring that the licence status of clinics is maintained.	In place - Paula Robinson
Precipitous decrease in funding due to large reductions in treatment undertaken because of Coronavirus. Note: as per FV1 this is a live issue, although treatment volumes recovered somewhat since spring 2020. Note: this risk may be both short and longer-term if clinics close down as a result.	As per FV1 risk - We have sufficient cash reserves to function normally for a period of several months if there was a steep drop-off in activity. The final contingency would be to seek additional cash and/or funding from the Department. We have agreed support for the remainder of 2020/21, and we will resume discussions about the likely impact on us in 2021/22 in the coming months.	In place – Richard Sydee Ongoing discussions as impact becomes clearer – Richard Sydee
Negative effects on staff wellbeing (both health and safety and mental health) caused by extended working from home (WFH), may mean that they are unable to work effectively, reducing overall staff capacity.	Provided equipment for staff who have to WFH without suitable arrangements in place. Ability of staff unable to work from home to work in Covid-19 secure office. Mental Health resources provided to staff, such as employee assistance programme and links to other organisations' resources. Mental Health First Aiders in place to increase awareness of need to care for mental health. Available to discuss mental health concerns confidentially with staff. Regular check-ins in place between staff and managers at all levels, to support staff, monitor effectiveness of controls and identify need for any corrective actions. Additional support for Managers in place. Corrective actions could include discussions about workload, equipment, reallocation of work or resource dependent on circumstance.	In place – Richard Sydee In place – Yvonne Akinmodun In place – Yvonne Akinmodun In place and ongoing – Yvonne Akinmodun
Inability of staff to return to office working may negatively impact organisational culture, reduce collaboration, or hamper working dynamics and productivity. Note: This risk will affect the organisation for some time including when we return to the office, while social distancing is in place and office working is significantly reduced due to Covid-19 restrictions. The ongoing consideration of this	Discussion about return to office working at CMG to ensure that this is planned effectively, and impacts considered. This is occurring on a month-by-month basis in the run up to returning to the office. Online solutions to maintain collaboration and engagement, such as informal team engagement and 'teas', Microsoft Teams etc.	Ongoing – Peter Thompson In place – Heads

Causes / sources	Controls	Status/Timescale / owner
risk is reflected within the OM1 risk.		
Risk that we miss posted financial, OTR or other correspondence.	Arrangement in place to securely store, collect and distribute post. Updated website info to ask people to contact us via email and phone. We notified all suppliers about the change in arrangements. Although this is unlikely to stop all post as some have automated systems.	In place– Richard Sydee In place – Jo Triggs In place – Morounke Akingbola
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
In common risk		
DHSC: HFEA costs exceed annual income because of reduced treatment volumes. Live issue as at April – captured under FV1	Use of cash reserves, up to appropriate contingency level available. The final contingency would be to seek additional cash and/or funding from the Department. (additional Grant in Aid has been provided for the 2020/2021 business year).	Richard Sydee

Reviews and revisions

09/06/2021 – SMT review – June 2021

SMT reviewed all risks, controls and scores and made the following points in discussion:

- Throughout the risk register, text had been edited to ensure that the risks were expressed in an active, current way (avoiding hypotheticals)
- RF1: Regulatory framework – Updated to reflect the latest position with regard to inspections.
- I1: Information provision – updated throughout.
- P1: Positioning and influencing – SMT considered that there were no additional interdependencies at present, but would keep this under review.
- C1: Capability – Discussed the recent increase in turnover, but decided that overall residual risk score should remain unchanged for now. Staff churn and its consequences are discussed in the risk commentary.
- OM1: Operating model – Updated to reflect the current position in 2 Redman Place, while also acknowledging that forthcoming Government guidance may necessitate further such updates. It is not yet clear when social distancing will be relaxed to the extent that smaller meeting rooms can be used, and an AV solution for the larger meeting rooms has not yet been installed.
- LC1: Legal challenge – Likelihood score increased to 3 (from 2), as a result of a pre-action letter. This increases the overall risk score to 12 (high), putting it at tolerance.

12/05/2021 - Authority review – May 2021

The Authority made no changes to the scores, and noted or discussed the following:

- Noted that the executive intend to review the wider risk management approach in the coming months.
- I1: Information provision – A further addition to potential risk causes was suggested, that the HFEA could be perceived as less consumer-focused, or out of step with other modern regulators, in the area of transparency about inspection findings.
- P1: Positioning and influencing – Whether we were influencing optimally, and whether there could be scope to act as a sector leadership convenor on certain matters. Further interdependencies could perhaps be reflected over time.
- C1: Capability – It was hoped we could act swiftly to facilitate mentoring and other such arrangements jointly with other ALBs in 2 Redman Place.
- The reassessment of risk C2, which was above tolerance, was noted.

19/04/2021 – SMT review – April 2021

SMT reviewed all risks, controls and scores and made the following points in discussion:

- SMT noted there were no substantive changes to the CS1, C1, RF1, LC1, I1 or P1 risks.
- FV1: Financial viability – The Director of Finance and Resources noted that we had had confirmation of our budget from the Department and finance team monitoring suggested the income risk for this business year was small. SMT agreed that the Risk and Business Planning Manager and Director of Finance and Resources should review the commentary to reflect updates, but there was no change in the score.
- C2: Board capability – SMT discussed the upcoming conversation with the Chair about plans for handling of Board member recruitment. SMT agreed that following that meeting, a full revision could be done to this risk by the Risk and Business Planning Manager and the Chief Executive to reflect these plans and AGC's earlier comments. On review, following discussion with the Chair the risk was revised per AGC's suggestion to include senior executive leadership risks and the score was raised.
- OM1: Operating Model – SMT discussed some updates from the central DHSC Office Move Programme which was coming to an end. The Director of Finance and Resources noted an update would be given to the Corporate Management Group on the remaining actions in May.
- CV1: Coronavirus – Given we are operating very well with virtual meetings, the inability of running in-person events was not causing risk to current strategic delivery so this risk cause was removed. There was no change to the score.

16/03/2021 - AGC review - March 2021

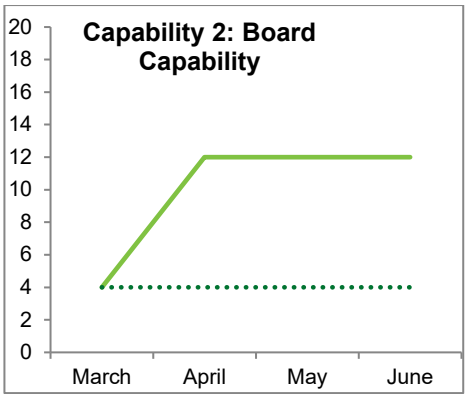
AGC reviewed all risks, controls and scores and made the following points:

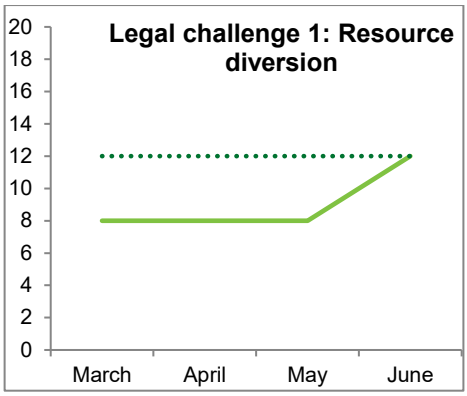
- AGC noted the four risks that had been reduced and that this seemed appropriate given the status of controls.
- Members suggested reframing the C2 risk now that there was more stability on Board recruitment, to reflect the key concern of managing knowledge retention and consistency. The risks associated with possible turnover within the Senior Management Team should also be reflected.
- Members raised questions about the OTR risk, DNA testing and the hybrid inspection regime.
- AGC noted the proposal to review the risk management policy, approach, and register, with this returning to AGC in October before going to the Authority in November. Members suggested a more dynamic approach could add value for the Strategic Risk Register.

Risk trend graphs (last updated June 2021)

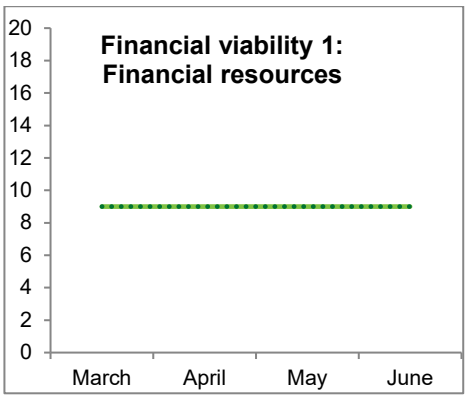
High and above tolerance risks

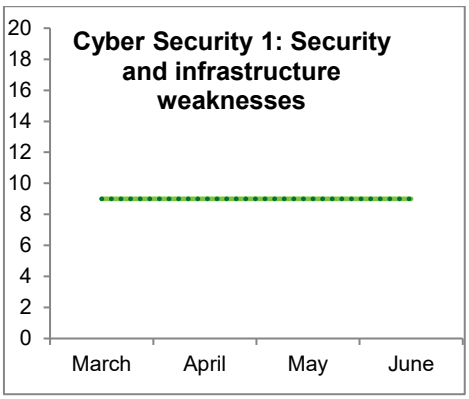
Key:

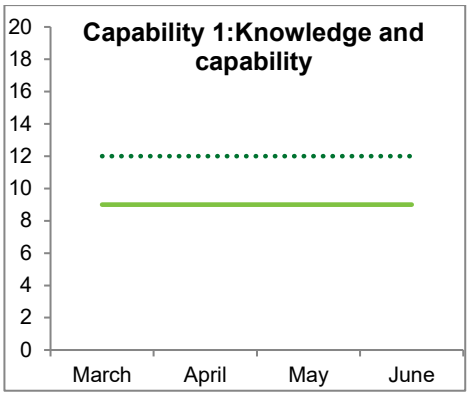


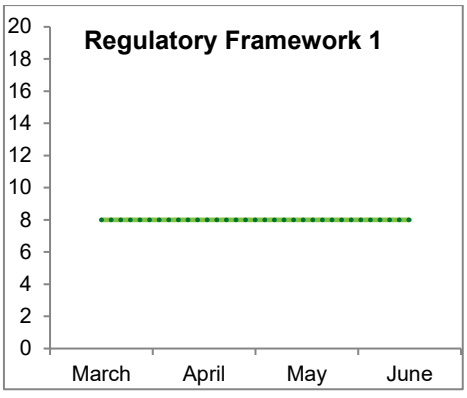


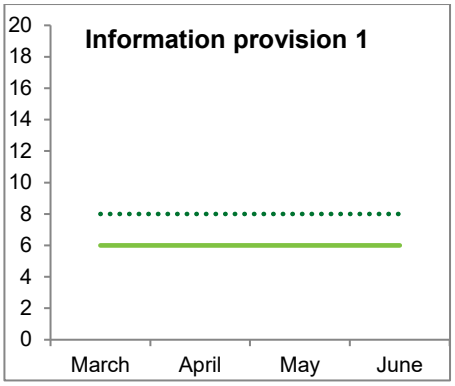
Lower and below tolerance risks

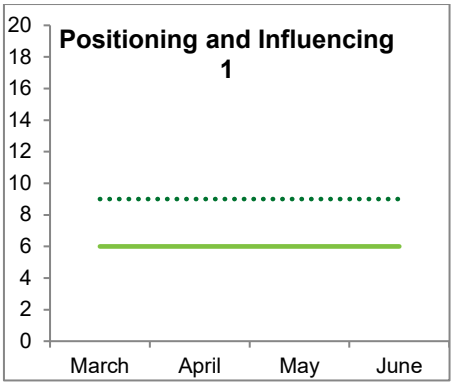


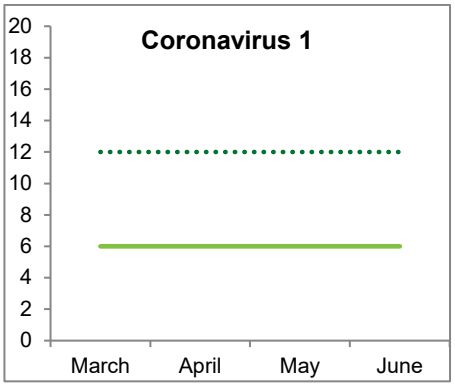







Information provision 1
20
18
16
14
12
10
8
6
4
2
0
March
April
May
June


Positioning and Influencing 1
20
18
16
14
12
10
8
6
4
2
0
March
April
May
June


Coronavirus 1
20
18
16
14
12
10
8
6
4
2
0
March
April
May
June

Criteria for inclusion of risks

Whether the risk results in a potentially serious impact on delivery of the HFEA's strategy or purpose.

Whether it is possible for the HFEA to do anything to control the risk (so external risks such as weather events are not included).

Rank

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

Risk trend

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

Risk scoring system

We use the five-point rating system when assigning a rating to the likelihood and impact of individual risks:

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

Risk scoring matrix

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

Risk Score = Impact x Likelihood

Likelihood

Risk appetite and tolerance

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

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

Assessing inherent risk

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

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

System-wide risk interdependencies

We explicitly consider whether any HFEA strategic risks or controls have a potential impact for, or interdependency with, the Department or any other ALBs. There is a distinct section beneath each risk to record any such interdependencies, so 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.

Human Resources update June 2021

Strategic delivery:	☒ Safe, ethical, effective treatment	☒ Consistent outcomes and support	☒ Improving standards through intelligence
Details:	**Human Resources Update June 2021**		
Meeting	Audit Committee Paper		
Agenda item	11		
Paper number	[AGC (22/06/2021) YA]		
Meeting date	22 June 2021		
Author	Yvonne Akinmodun, Head of Human Resources		
Output:			
	For Information		
Recommendation	The Committee is asked to note and comment on the: a. preparations made for the return to office working (section 2); and b. work on employee wellbeing (section 4 and annex A)		
Organisational risk	☐ Low	☒ Medium	☐ High

1. Introduction

1.1. This paper sets out the some of the key HR activities the organisation has been working on in relation to preparing for the return to office working (section 3) and staff wellbeing (section 4 and annex A) over the last six months. It begins with an overview of the key HR statistical measures (section 2, turnover and sickness).

2. HR Statistics

2.1. Average turnover in the last 12 months remains low at 11.5%. We do however anticipate a slight increase in turnover as the job market shows signs of recovery. The impact of the government's decision not to award a pay rise to public sector workers may also affect our turnover figures in the next 12 months.

2.2. Turnover is not evenly spread across the organisation. We have seen higher turnover in the policy and information management teams, due to a combination of maternity leave, temporary contracts and in the case of IT, opportunities elsewhere. We will continue to monitor turnover across the board and try to ensure appropriate support is in place to mitigate any impact with measures such as offering internal promotion and opportunities for acting up to staff.

2.3. We will also continue to conduct exit interviews with those who are leaving the organisation to understand what lessons can be learned to help us continually improve engagement in the workplace.

2.4. The average rate of sickness absence in the last 6 months is 1.74%. This is below the civil service average. It should be noted that we have seen limited impact of COVID on sickness absence figures with, thankfully, only one recorded case of long COVID. We will continue to monitor and offer support in such cases.

3. Preparing to return to office working

3.1. Since the government's publication of the COVID recovery roadmap earlier this year, we have set about creating guidance and advice to staff and managers on our approach to a return to office working.

3.2. We are approaching the return to office working in phases. The first phase is timed to begin once the government makes a decision that the final stage of lockdown can be lifted (previously from 21 June, now from 19 July). From the start of June, we have been encouraging staff to visit the office on an ad hoc basis as a way to encourage the gradual return to working from the office.

3.3. So far, 33 members of staff have visited the office at least once in the last 3 months with some making regular visits up to 2 – 3 times a week.

3.4. Looking ahead, we are planning to move to a form of hybrid working.

4. Wellbeing

4.1. Our staff, like many, have been working from home for over 18 months. We have been able to provide a range of tools and support to staff to help them manage with some of the challenges associated with full time homeworking.

4.2. The paper attached at annex A was prepared for a recent audit and sets out the activities and actions we have put in place over the last year to help support staff wellbeing during the various periods of lockdown.

4.3. We are also working on providing additional information to support managers so they feel confident in managing their teams as we transition to hybrid working.

5. Recommendations

- The Committee is asked to note and comment on the actions taken to date.

Health and Wellbeing at the HFEA

Introduction

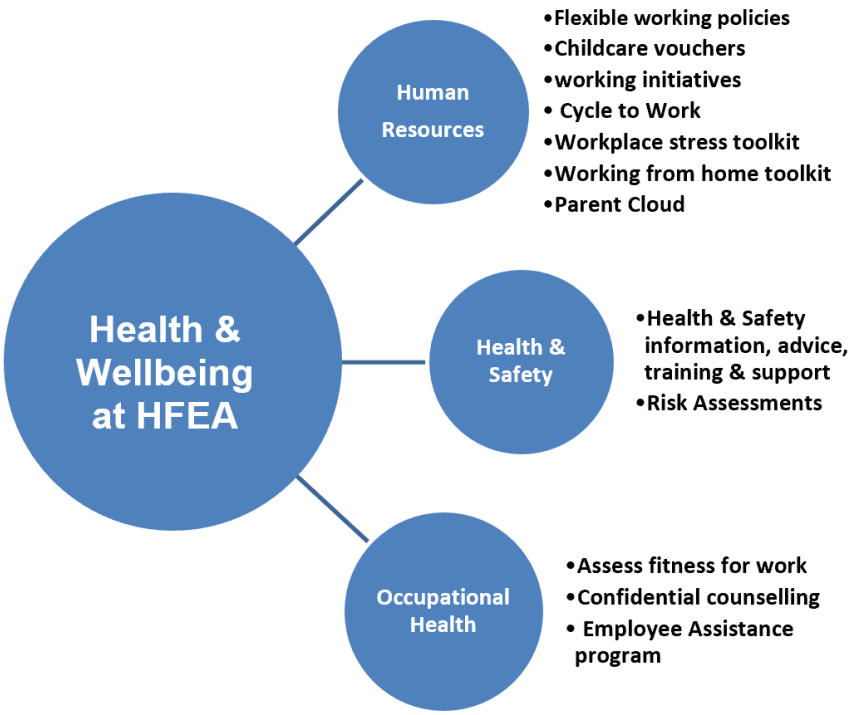
Our staff are our most important asset in delivering our commitment to ensure that everyone who steps into a fertility clinic, and everyone born as a result of treatment, receives high quality care. In order to do so, it is important that our staff are fit, healthy and able to do the work we ask of them.

Having a workplace and a workforce that is healthy is central to ensuring an effective and efficient organisation in which staff feel cared for, supported and valued.

1. Current Practice

Figure 1 provides a summary of the range of policies, services and programmes that are currently available for staff.

1.1.



1.2. In addtion to formal policies, the HFEA has also introduced a range of social and health activities such as:

- Training courses for managers on managing remote teams
- Mental Health First aider support
- Bi-weekly quizzes
- Quarantea – Informal virtual coffee/tea get togethers
- Remote all staff get togethers
- A one off additional half day's leave at christmas
- The introduction of a parenting platform – Parent Cloud to support working parents dring and after lockdown
- Free flu jabs offered to all employees requesting one

2. Impact of COVID on wellbeing at work

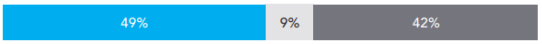
2.1. In March 2020, HFEA, like most organisations in the country moved to full time virtual working. To support this approach, staff where asked to provide a list of any equipment they might need to support remote working

2.2. Managers were provided with training to ensure they are able to manage teams remotely along with a toolkit of tips and ideas to ensure a smooth transition to the new ways of working

2.3. In April 2020, we created a health and wellbeing toolkit for managers to help guide them in managing the health and wellbeing of their team members

2.4. In June 2020, we conducted a survey to find out from staff their thoughts on remote working and also to identify what additional support they might need. Below is a summary of staff feedback:

Theme Report - How we can support you during the Coronavirus crisis

Selected Theme/Focal Point	Response favourability
How we can support you during the Coronavirus crisis	

How we can support you during the Coronavirus crisis questions

Impact	Question	Theme	Response favourability
	If I had a concern about returning to work, I know how to raise it	How we can support you during the Coronavirus crisis	
	If our offices / sites were open today, I would prefer to work there	How we can support you during the Coronavirus crisis	

2.5. Since conducting the survey, we have been able to offer optional office working, initially at CQC offices in Victoria, prior to our move to our new offices in Stratford.

2.6. In February 2021, following the government's publication of a roadmap, staff have been given the option to work from the Stratford office. We have seen notable take up, in particular with some individuals seeking to work from the office on a full time basis

3. Sickness absence

3.1. 17 days were recorded as sickness absence due to stress/mental health over the last year, resulting in 1 occupational health referral

3.2. The HFEA has a sickness absence policy, which provide guidance and support for managers and staff on how to manage sickness absence.

3.3. The policy also provides and overview of support offered in the form of occupational health referrals and use of our employee assistance program.

4. Stress management

4.1. The HFEA launched a stress management policy along with a manager's guide and toolkit in 2019. The policy is accompanied by tools such as self-assessment tools to help individuals identify symptoms of workplace stress.

5. Covid and Health and Safety

5.1. All staff attending the office at Redman Place are required to complete a Covid risk assessment and adhere to the HFEA lone working policy.

5.2. Desks are prebooked to monitor staff number in line with social distancing requirements

5.3. Masks and lateral flow testing are commended before attending the office recommended

6. Training to support wellbeing

6.1. In June 2020, the organisation moved to an online learning platform for the delivery of its training. Some of the training available is in place to support wellbeing.

6.2. Below is a list of online courses provided to support wellbeing at work

- Remote working (mandatory for all staff)
- Managing personal stress (mandatory for all staff)
- Managing stress in your team (for managers)
- Managing remote teams (for managers)
- Growing your resilience (10 employees)
- Understanding you (8 employees)

7. Wellbeing post covid

7.1. As we emerge from lockdown, we recognise that we may choose to adopt different ways of working, such as hybrid working for most of our staff

7.2. We are working on putting guidance in place to ensure managers look out for their staff by:

- maintaining regular contact and not restricting check-ins to work activity
- ensuring staff are clear what work they should be undertaking
- being alert to and aware of the various signs of stress
- arranging meetings for 25 or 55 minutes to ensure comfort breaks between meetings
- ensuring regular screen breaks are taken
- addressing with staff any concerns they have about their home working environment or their ability to work from home
- ensuring that staff do not work excessive hours and feel obliged to keep mobile phones and laptops on when they have stopped working.

7.3. We will also encourage staff to take steps to look after their wellbeing during days working from home. This includes:

- maintaining regular contact with their manager and colleagues
- taking regular breaks
- avoiding being ‘always on’ by identifying non-working time and switching off laptops and mobiles
- contacting the Employee Assistance Programme or a Mental Health First Aider if they need support
- being aware of personal and workplace stressors and the activities and resources which can help to address these.

7.4. In recognition of the fact that home working may not be suitable for all staff, managers will be asked to accommodate requests to work exclusively in the office where home working is not appropriate for wellbeing reasons.

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	12
Paper number	AGC (22/03/2021) DH
Meeting date	22 June 2021
Author	Dan Howard, Chief Information Officer
Output:	
For information or decision?	For information
Recommendation	The Committee is asked to note: • Progress made with the laptop replacement programme and approach for the disposal of redundant equipment • That our annual internal IT security review will take place in July • Our plan for the upgrade of our electronic management system shortly, the arrangements for PRISM go-live support and use of the new office The committee is asked to approve: • The annual Data Security and Protection Toolkit assessment, as set out in section 4.2 and Annex A
Resource implications	Within budget
Implementation date	Ongoing
Communication(s)	Regular, range of mechanisms
Organisational risk	☐ Low ☒ Medium ☐ High
Annexes:	Annex A – Data Security and Protection Toolkit annual assessment

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. This paper provides an update on IT infrastructure and cyber security relating to our laptop replacement programme, our planned upgrade to our electronic management system, IT security review, IT ticket system and update relating to IT infrastructure associated with the new office.

1.3. Our Data Security and Protection Toolkit final submission for 2021 is due to be submitted at the end of June. As previously indicated to AGC, our proposed submission will be 'not met' as we will meet 32 of the 37 requirements by the end of June. This paper sets out the proposed submission, our arrangements for audit and requests AGC to approve the annual submission.

2. Infrastructure improvements

Replacement laptops

2.1. In March we reported to AGC that we had reviewed our laptop estate along with support calls associated with hardware issues. Our laptop replacement programme is due to conclude shortly and all laptops older than 42 months are being replaced. 26 have been replaced and the remaining 3 will be replaced in the coming weeks. As a result of the refresh programme the number of support tickets raised for hardware issues have reduced in recent months.

Redundant device disposal

2.2. All redundant devices which have been replaced will be securely disposed of through our agreed disposal process and via our IT hardware disposal partner, Stone Computers.

2.3. Data bearing items are subject to secure data erasure to HMG Information Assurance Standard number 5 (HMG level 5) using market-leading Blancco software which is approved by the Communication Electronics Security Group (CESG).

IT security review

2.4. Our annual IT technical security review will take place during July. It will be an interactive session involving key HFEA staff.

2.5. The review will consider current and future business requirements, IT security policies and technical architecture. It will also be a review of data and systems, access, and the implementation and management of any necessary further controls commensurate with risk.

PRISM go-live support

2.6. Our IT support ticket system is being configured to add support queues and accounts so that PRISM support tickets can be triaged and managed effectively when the PRISM system is launched.

IT services in Redman Place

2.7. Around 50% of HFEA staff have worked from Redman Place so far. Staff have reported a positive experience to date. A small number of residual issues are being addressed with

partners such as shared printing (CQC) and Audio Visual services in the larger shared meeting rooms (NICE).

3. Document Management system upgrade

3.1. We will shortly be upgrading our electronic document management system (Content Manager) to an updated version (v10).

3.2. The new version is a significant improvement on the current version. It is used through an internet browser rather than a locally installed application. Engagement sessions with key users have started and a project will commence shortly.

3.3. The new system will be installed, configured and launched by the end of August 2021.

4. Data Security and Protection Toolkit (DSPT)

Background

4.1. AGC will recall that the Data Security and Protection Toolkit (DSPT) is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's ten data security standards. It the first time we have submitted an end of year annual DSPT return.

4.2. As a reminder, the DSPT sets both mandatory and non-mandatory requirements. There are 42 detailed requirements and 37 of them are mandatory. We will assess ourselves against the 37 mandatory requirements only.

4.3. Each requirement has multiple questions for which we need to provide evidence and explanation, the total number of evidence items across the 37 mandatory requirements is 88.

4.4. The DSPT is completed on an annual basis. Assessment is in two stages; a mid-year baseline assessment and a final submission in June 2021 (extended from March 2021 due to the Covid pandemic).

4.5. AGC will recall that we submitted our mid year interim assessment in February 2021 and at the time we forecast that we would not be fully compliant with the mandatory DSPT requirements for the annual submission in June 2021.

4.6. For our interim submission, we met 31 out of the 37 mandatory requirements.

4.7. This remainder of this paper sets out our proposed June 2021 assessment for approval by AGC ahead of submission.

Audit and assurance

4.8. An audit by GIAA is currently taking place assessing the adequacy of our evidence against the below subset of assertions. GIAA will not audit the assertion where the evidence is not yet available or where we have assessed ourselves as not meeting it.

1.6	The use of personal information is subject to data protection by design and by default.
1.8	There is a clear understanding and management of the identified and significant risks to sensitive information and services
2.2	Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.

3.1	There has been an assessment of data security and protection training needs across the organisation.
4.2	Organisation assures good management and maintenance of identity and access control for its networks and information systems.
5.1	Process reviews are held at least once per year where data security is put at risk and following data security incidents.
6.2	All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.
7.2	There is an effective test of the continuity plan and disaster recovery plan for data security incidents.
7.3	You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.
8.3	Supported systems are kept up-to-date with the latest security patches.

4.9. We will take any necessary action as identified by the audit ahead of the end-June submission deadline for the assertions that we have confirmed we will meet.

June 2021 submission

4.10. We have assessed ourselves as meeting 32 out of the 37 mandatory requirements. This means that our submission, as reported to AGC in March 2021, will be 'not met'.

4.11. We believe there are no significant consequences of a 'not met' return. That is because this is our first annual submission, we have made substantial progress to date, we have an improvement action plan in place and because clinics are mandated to provide treatment data to us in accordance with the HFEA Act.

4.12. The table below provides our action plan including the detail of the five assertions we will not meet. It sets out the assertion, the evidence required, the reason we will not meet it and the timeline for completion.

Assertion	Evidence item	Details	Action, owner, deadline.
1.6 The use of personal information is subject to data protection by design and by default	1.6.4 Provide the overall findings of the last data protection by design audit (Should be from last 12 months - covering access control, encryption, computer port control, pseudonymisation and physical control)	We don't have the results from a data protection by design audit carried out in the past 12 months which covers the requirements for this assertion as a full penetration test has not been carried out during the past 12 months. We don't routinely pseudonymise any data held on the HFEA server	Undertake full network penetration test covering this assertion; IT Systems Manager; December 2021

		as its either deleted according to our Retention Schedule or we need to identify individuals for Register enquires such as OTR. Physical control checks are completed by the Facilities management which is headed by NICE. The IT Systems Manager will be carrying out a penetration test meeting this requirement by the end of the 2021 calendar year. For this assertion we will provide results from our full network penetration test when it has been completed.	
1.7 Effective data quality controls are in place and records are maintained appropriately	1.7.2 Was the scope of the last data quality audit in line with guidelines (In accordance to Service User Data Audit)	The Service User Data Audit requires checking health record data for accuracy. The health record data we retain is Register data and the service we provide this data for is Opening the Register. This is not a typical health care service similar to other parts of the healthcare sector. We cannot comply with the strict definition of this requirement as the Service User Data Audit does not relate to HFEA fertility data or our work as a regulator. We don't provide a health care service to patients and so we will continue to discuss this requirement with NHS Digital.	Through discussions with NHS Digital we are seeking agreement on flexibility of interpretation for our next DSPT submission in 2022 so that evidence of our data quality controls and National Audit Office records audit can be used as evidence to show we meet the principle of this assertion.

3.4 Leaders and board members receive suitable data protection and security training	3.4.1 Have your SIRO and Caldicott Guardian received appropriate data security and protection training?	Due to changes in the Information team the newly appointed Head of Information will undertake the Caldicott Guardian training. The SIRO (Senior Risk Information Officer – Director of Finance and Resources) has arranged for training with HR which will be completed after June deadline	Complete Caldicott training; Head of Information (not yet recruited); end Dec 2021 Complete SIRO training; Director of Finance and Resources; end Sept 2021
3.4 Leaders and board members receive suitable data protection and security training	3.4.2 What percentage of Board Members have completed appropriate data security and protection training?	Authority members completed training around a year ago. The Head of Planning and Governance will arrange refresher training by end September 2021 (suitable courses have been identified).	Arrange training; Head of Planning and Governance; end September 2021
6.2 All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway	6.2.11 You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) records in place for their domain to make email spoofing difficult	This detailed level of enforcement is not currently in place. These controls will be put in place by September 2021.	Implement necessary controls, IT Systems Manager; September 2021
9.2 A penetration test has been scoped and undertaken	9.2.2 The date the penetration test was undertaken	The last full penetration test was completed before April 2020 and so cannot be used as evidence for this assertion. As set out in the response to 1.6.4, the next full penetration test will take place by December 2021.	Undertake full network penetration test covering this assertion; IT Systems Manager; December 2021

4.1. See Annex A for our proposed assessment:

- Items marked as 'completed' are complete and we will collate the evidence and store centrally
- Items marked as 'pending' are due to be completed shortly (before the end of June 2021) and the evidence will be stored centrally
- Items marked as 'Not met' are assertions where we will not fully meet the requirement by the end June 2021

4.2. AGC are requested to:

- Note the proposed submission in Annex A
- Note the action plan in 4.12 above
- Note that when we receive the results of the audit we will take any necessary action as identified by the audit ahead of the end-June submission deadline
- Approve the DSPT annual submission as set out in Annex A, specifically that we meet 32 of the 37 mandatory requirements and our submission is 'not met'.
- Authorise the Information Governance and Records Manager to submit the assessment on the NHS Digital website before the end of June.

5. Recommendation

The Committee is asked to note:

- Progress made with the laptop replacement programme and approach for the disposal of redundant equipment
- That our annual internal IT security review will take place in July
- Our plan for the upgrade of our electronic management system shortly, the arrangements for PRISM go-live support and use of the new office

The committee is asked to approve:

- The annual Data Security and Protection Toolkit assessment, as set out in section 4.2

1. Annex A – Data Security and Protection Toolkit interim assessment

Assertion	Progress
1.1.1 Has SIRO responsibility for data security been assigned?	Completed
1.1.2 List the names and job titles of your key staff with responsibility for data protection and/or security	Completed
1.1.3 Are there clear lines of responsibility and accountability to named individuals for data security?	Completed
1.1.4 Is data security direction set at board level and translated into effective organisational practices?	Completed
1.2.1 Are there board approved data security and protection policies in place that follow relevant guidance	Completed
1.2.3 How are data security and protection policies made available to the public	Completed
1.3.1 What is your ICO registration number?	Completed
1.3.2 How is transparency information (e.g. privacy notice) published and available to the public?	Completed
1.3.5 Have there been any ICO actions taken against the organisation in the last 12 months, such as fines, enforcement notices or decision notices?	Completed
1.4.1 Provide details of the record or register that details each use or sharing of personal information	Completed
1.4.2 When did your organisation last review both the list of all systems/information assets holding or sharing personal information and data flows?	Completed
1.4.4 Provide a progress update on your compliance with the national data opt-out	Completed
1.5.2 Does your organisation carry out regular data protection spot checks?	Completed
1.6.1 There is an approved procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements	Pending
1.6.2 There are technical controls that prevent information from being inappropriately copied or downloaded	Completed
1.6.3 Briefly describe the physical controls your buildings have that prevent unauthorised access to personal data	Completed
1.6.4 Provide the overall findings of the last data protection by design audit (Should be from last 12 months - covering access control, encryption, computer port control, pseudonymisation and physical control)	Not met
1.7.2 Was the scope of the last data quality audit in line with guidelines (In accordance to Service User Data Audit)	Not met (see 4.12)
1.7.4 Has a records retention schedule been produced?	Completed
1.7.5 Provide details of when personal data disposal contracts were last reviewed/updated	Completed
1.8.1 Does your organisation operate and maintain a data security risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility?	Completed

1.8.3 What are your top three data security and protection risks?	Completed
2.2.1 Is there a data protection and security induction in place for all new entrants to the organisation?	Completed
2.2.2 Do all employment contracts contain data security requirements?	Completed
3.1.1 Has an approved organisation-wide data security and protection training needs analysis been completed after 1 April 2020?	Pending
3.2.1 Have at least 95% of all staff, completed their annual data security awareness training in the period 1 April 2019 to 30 Sep 2020	Completed
3.3.1 Provide details of any specialist data security and protection training undertaken	Completed
3.3.2 The organisation has appropriately qualified technical cyber security specialist staff and/or service	Completed
3.3.3 The organisation has nominated a member of the cyber associates network	Completed
3.4.1 Have your SIRO and Caldicott Guardian received appropriate data security and protection training?	Not met
3.4.2 What percentage of Board Members have completed appropriate data security and protection training?	Not met
4.1.1 Your organisation maintains a record of staff and their roles	Completed
4.1.2 Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?	Completed
4.2.1 When was the last audit of user accounts held?	Completed
4.2.5 Are unnecessary user accounts removed or disabled	Completed
4.3.1 All system administrators have signed an agreement which holds them accountable to the highest standards of use	Completed
4.3.2 Are users, systems and where appropriate, devices, always identified and authenticated prior to being provided access to information or system?	Completed
4.4.1 Has the Head of IT, or equivalent, confirmed that IT administrator activities are logged and those logs are only accessible to appropriate personnel?	Completed
4.4.3 The organisation does not allow users with wide ranging or extensive system privilege to use their highly privileged accounts for high-risk functions, in particular reading email and web browsing	Completed
4.5.4 Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and shall not be easy to guess. Passwords which would on their own grant extensive system access, should have high strength	Completed
5.1.1 Root cause analysis is conducted routinely as a key part of your lessons learned activities following data security incident	Completed
5.1.2 Provide summary details of process reviews held to identify and manage problem processes which cause security breaches	Completed
6.1.1 A data security and protection breach reporting system is in place	Completed
6.1.4 How is the Board or equivalent notified of the action plan for all data security and protection breaches?	Completed
6.1.5 Individuals affected by a breach are appropriately informed	Completed
6.2.2 Number of alerts recorded by the anti virus tool in the last 3 months	Completed
6.2.3 Has antivirus/anti-malware software been installed on all computers that are connected to or capable of connecting to the Internet	Completed
6.2.11 You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) records in place for their domain to make email spoofing difficult	Not met

6.2.12 You have implemented spam and malware filtering, and enforce DMARC on inbound email	Completed
6.3.1 If you have had a data security incident, was it caused by a known vulnerability?	Completed
6.3.2 The organisation has responded to high severity CareCERT alerts within 48 hours over the last 12 months	Completed
6.3.3 The organisation has a proportionate monitoring solution to detec cyber events on systems and services	Completed
6.3.5 Are all new Digital services that are attractive to cyber criminals for the purposes of fraud, implementing transactional monitoring techniques from the outset?	Completed
7.1.1 Organisations understand the health and care services they provide	Completed
7.1.2 Do you have well defined processes in place to ensure the continuity of services in the event of a data security incident, failure or compromise?	Completed
7.2.1 Explain how your data security incident response and management plan has been tested to ensure all parties understand their roles and responsibilities as part of the plan	Pending
7.2.4 From the business continuity exercise which issues and actions were documented, with names of actionees listed against each item	Completed
7.3.1 On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary	Completed
7.3.2 All emergency contacts are kept securely, in hardcopy and are up-to-date	Pending
7.3.4 Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed	Completed
8.1.1 Provide evidence of how the organisation tracks and records all software assets and their configuration?	Completed
8.1.2 Does the organisation track and record all end user devices and removeable media assets?	Completed
8.2.1 List of unsupported software prioritised according to business risk, with remediation plan against each item	Completed
8.2.2 The SIRO confirms that the risks of using unsupported systems are being treated or tolerated	Completed
8.3.1 How do your systems receive updates and how often?	Completed
8.3.2 How often, in days, is automatic patching typically being pushed out to remote endpoints?	Completed
8.3.3 There is a documented approach to applying security updates (patches) agreed by the SIRO	Completed
8.3.4 Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.	Completed
8.4.1 Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?	Completed
8.4.2 All infrastructure is running operating systems and software packages which are patched regularly, and as a minimum in vendor support.	Completed
9.1.1 The Head of IT, or equivalent role confirms all networking components have had their default passwords changed	Completed
9.2.1 The annual IT penetration testing is scoped in negotiation between the SIRO, business and testing team including checking that all networking components have had their default passwords changed	Completed
9.2.2 The date the penetration test was undertaken	Not met
9.3.1 All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities	Completed
9.3.3 The organisation uses the UK Public Sector DNS Service to resolve internet DNS queries	Completed

9.3.4 The organisation ensures that changes to your authoritative DNS entries can only be made by strongly authenticated and authorised administrators	Completed
9.3.5 The organisation understands and records all IP ranges in use across your organisation	Completed
9.3.6 The organisation is protection data in transit (including email) using well configured TLS v1.2 or better	Completed
9.3.7 The organisation has registered and uses the National Cyber Security Centre (NCSC) Web Check service for your publicly visible applications	Completed
9.4.4 Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way	Completed
9.4.6 What level of assurance did the independent audit of your data security and protection toolkit provide to your organisation	Completed
9.6.1 All devices in your organisation have technical controls which manage the installation of software on the device	Completed
9.6.2 Confirm all data is encrypted at rest on all mobile devices and removeable media and you have the ability to remotely wipe and/or revoke access from an end user device	Completed
9.6.10 You have a plan for protecting devices that are natively unable to connect to the Internet, and the risk has been assessed, documented, accepted and signed off by the SIRO	Completed
9.7.1 Have one or more firewalls (or similar network device) been installed on all the boundaries of the organisation's internal network(s)	Completed
10.1.1 The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration	Completed
10.2.1 Organisations ensure that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification	Completed
10.2.2 Organisations should, as part of their risk assessment, determine whether the supplier certification is sufficient assurance	Completed
10.2.4 Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility	Completed

Audit and Governance Committee Forward Plan

Strategic delivery:	☐Safe, ethical, effective treatment	☐Consistent outcomes and support	☒Improving standards through intelligence
Details:			
Meeting	Audit & Governance Committee Forward Plan		
Agenda item	13		
Paper number	AGC (22/06/2021) MA		
Meeting date	22 June 2021		
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 Forward Plan		
Resource implications	None		
Implementation date	N/A		
Organisational risk	☒ Low	☐ Medium	☐ High
	Not to have a plan risks incomplete assurance, inadequate coverage or unavailability key officers or information		
Annexes	N/A		

Audit & Governance Committee Forward Plan

AGC Items Date:	8 Dec 2020	16 Mar 2021	22 Jun 2021	5 Oct 2021
Following Authority Date:	27 Jan 2021	24 Mar 2021	7 July 2021	17 Nov 2021
Meeting 'Theme/s'	Register and Compliance, Business Continuity	Finance and Resources (deferred to June)	Annual Reports, Information Governance, People	Strategy & Corporate Affairs, AGC review
Reporting Officers	Director of Compliance and Information	Director of Finance & Resources	Director of Finance & Resources	Director of Strategy and Corporate Affairs
Strategic Risk Register	Yes	Yes	Yes	Yes
Risk Management Policy[1]				Yes
Digital Programme Update	Yes	Yes	Yes	
Annual Report & Accounts (inc Annual Governance Statement)		Draft Annual Governance Statement –	Yes – For approval	
External audit (NAO) strategy & work	Audit Planning Report	Interim Feedback	Audit Completion Report	
Information Assurance & Security			Yes, plus SIRO Report	
Internal Audit Recommendations Follow-up	Yes	Yes	Yes	Yes
Internal Audit	Update	Update	Results, annual opinion approve draft plan	Update
Whistle Blowing, fraud (report of any incidents)	Update as necessary	Update as necessary	Update as necessary	Update as necessary

[1] Policy will have been reviewed by the Executive, including updated appetite statement for Authority approval.

AGC Items Date:	8 Dec 2020	16 Mar 2021	22 Jun 2021	5 Oct 2021
Public Interest Disclosure (Whistleblowing) policy		Reviewed annually thereafter		
Anti-Fraud, Bribery and Corruption policy		Reviewed and presented annually thereafter GovS: 013 Counter Fraud		
Contracts & Procurement including SLA management	Update as necessary	Update as necessary	Update as necessary	Update as necessary
HR, People Planning & Processes	Bi-annual HR report		Yes Including bi-annual HR report	
Strategy & Corporate Affairs management				Yes
Regulatory & Register management	Yes			
Cyber Security Training				Yes – update on whether annual training undertaken
Resilience & Business Continuity Management	Yes	Yes	Yes	Yes
Finance and Resources management		Yes		
Reserves policy				Yes
Estates	Yes	Yes	Yes	Yes
Review of AGC activities & effectiveness, terms of reference	Yes			
Legal Risks				Yes
AGC Forward Plan	Yes	Yes	Yes	Yes

AGC Items Date:	8 Dec 2020	16 Mar 2021	22 Jun 2021	5 Oct 2021
Session for Members and auditors	Yes	Yes	Yes	Yes

Gifts and Hospitality Register

Details about this paper

Area(s) of strategy this paper relates to:	The best care – effective and ethical care for everyone The right information – to ensure that people can access the right information at the right time Shaping the future – to embrace and engage with changes in the law, science and society		
Meeting	AGC		
Agenda item	14		
Paper number	HFEA (16/03/2021) MA		
Meeting date	22 June 2021		
Author	Morounke Akingbola (Head of Finance)		
Output:			
For information or decision?	For information		
Recommendation	Attached is the latest Gifts and Hospitality Register. Since the last meeting, **no items** have been added. Members are asked to note.		
Resource implications			
Implementation date	2021/22 business year		
Communication(s)			
Organisational risk	☐ Low	☒ Medium	☐ High

Register of Gifts / Hospitality Received and Provided/Declined

Version: HFEAG0001
Jun-21

DIVISION / DEPARTMENT: HFEA
FINANCIAL YEAR: 2019/20

	Details of the Gift or Hospitality						Provider Details			Recipient Details	
Type	**Brief Description of Item**	**Reason for Gift or Hospitality**	**Date(s) of provision**	**Value of Item(s)**	**Location where Provided**	**Action on Gifts Received**	**Name of Person or Body**	**Contact Name**	**Relationship to Department**	**Name of Person(s) or Body**	**Contact Name**
Either 'Provision' or 'Receipt'	*Give a brief description of the gift or hospitality recorded*	*Summarize the reason or occasion for the gift or hospitality*	*Give the date(s) on which it was provided or offered*	*Give the known or estimated value - if unknown then state 'unknown' and explain further under the 'Reason for Gift' column.*	*Give the name of the venue or location at which the gift or hospitality was provided*	*For Gifts Received only, specify what happened to the item(s) after it was received*	*Give the name of the individual or organization providing or offering the gift / hospitality*	*Give a contact name if an individual is not specified as the provider - otherwise leave blank*	*Specify the relationship of the provider to the Department (e.g. 'supplier', 'sponsor', etc.) - if the Department is the provider then leave blank*	*Give the name of the individual(s) or organisation receiving the gift / hospitality - if there are multiple recipients, specify each on a separate line*	*Give a contact name if an individual is not specified as the recipient - otherwise leave blank*
Receipt	Lunch invitation	To introduce to Legal Trainers	10/08/2017	£ -	Not known	Lunch accepted	Old Square Chambers	Eleena Misra	Legal Consultancy	HFEA	C Drennan
Receipt	Lunch invitation	Introduce Clients to new lawyers	01/11/2017	£ -	Not known	Lunch accepted	Blackstone Chambers	Catherin Callaghan	Legal Consultancy	HFEA	C Drennan
Receipt	Breakfast invitatoin	Breakfast meeting	08/02/2018	£ -	Not known	Breakfast accepted	Fieldfisher	Mathew Lohn	Legal Consultancy	HFEA	P Thompson
Receipt	Invitation to Silk Party	Informing Clients of a change (to QC)	22/03/2018	£ -	Not known	Invitation accpeted	Blackstone Chambers	Catherin Callaghan	Legal Consultancy	HFEA	C Drennan
Receipt	Lunch provided	Lunch provided prior to a review meeting	24/07/2019	£ 20.00	Not known	Lunch accepted	Alsicent		IT Support supplier	HFEA	D Howard
Receipt	Chocolates	Recruitment agency meeting	16/12/2019	£ -	Not known	Shared in office	Covent garden Bureau	Charlotte Saberter	Recruitment agency	HFEA	J Hegarty
Receipt	Lunch invitation	Interactive Workshops	11/12/2019	£	Central London	Lunch accepted	Interactive Workshop	Anna Beer	Training	HFEA	Y Akinmodun
Receipt	Cheque received	Book Review conducted	14/02/2020	£ 50.00	Not known	Cheque cashed donated to charity	Literary Review		None	HFEA	M Gilmore