Audit and Governance Committee meeting - agenda

18 June 2019

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

	Agenda item		Time
1.	Welcome, apologies and declaration of interests		10:30am
2.	Minutes of 5 March 2019 **[AGC (18/06/2019) 670 DO]**	For Decision	10.35am
3.	Minutes of 8 May 2019 **[AGC (18/06/2019) 671 DO]**	For Decision	10.40am
4.	Matters Arising **[AGC (18/06/2019) 672 MA]**	For Information	10.45am
5.	Internal Audit a) Annual Assurance Statement 2018-19 **[AGC (18/06/2019) 673 TS]** b) 2019/20 Plan **[AGC (18/06/2019) 674 TS]**	 For Information For Information	10.55am
6.	Progress with Audit Recommendations **[AGC (18/06/2019) 675 MA]**	For Information	11.15am
7.	Draft Annual Report and Accounts **[AGC (18/06/2019) 676 RS]**	For Approval	11.25am
8.	External Audit – Audit Completion Report **[AGC (18/06/2019) 677 NAO]**	For Information	11.45am
9.	Human Resource update 2019 **[AGC (18/06/2019) 678 YA]**	For information	12.00pm
10.	Estates Update **[AGC (18/06/2019) 679 RS]**	Verbal update	12.15pm
11.	Digital Programme Update **[AGC (18/06/2019) 680 DH]**	For Information	12.25pm

12.	Resilience, Business Continuity Management Cyber Security **[AGC (18/06/2019) 681 DH]**	For Information	12.35am
13.	Strategic Risk Register **[AGC (18/06/2019) 682 HC]**	For Comment	12.45pm
14.	AGC Forward Plan **[AGC (18/06/2019) 683 MA]**	For Decision	1.00pm
15.	Whistle Blowing and Fraud **[AGC (18/06/2019) 684 RS]**	For Comment	1.10pm
16.	Contracts and Procurement **[AGC (18/06/2019) 685 MA]**	Verbal update	1.25pm
17.	Any other business		1.35pm
18.	Close (Refreshments & Lunch provided)		1.40pm
19.	Session for members and auditors only		1.45pm

Next Meeting: 10am Tuesday, 8 October 2019, Chartered Institute of Arbitrators, 12 Bloomsbury Square, London, WC1A 2LP

Audit and Governance Committee meeting minutes

Strategic delivery:	☐ Setting standards	☐ Increasing and informing choice	☐ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item	2		
Paper number	AGC (18/06/2019) 670		
Meeting date	18 June 2019		
Author	Debbie Okutubo, Governance Manager		
Output:			
For information or decision?	For decision		
Recommendation	Members are asked to confirm the minutes as a true and accurate record of the meeting		
Resource implications			
Implementation date			
Communication(s)			
Organisational risk	☒ Low	☐ Medium	☐ High
Annexes			

Minutes of Audit and Governance Committee (AGC) meeting held on 5 March 2019

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

Members present	Anita Bharucha (Chair) Margaret Gilmore Mark McLaughlin Geoffrey Podger
Apologies	Samantha Hayhurst, Department of Health and Social Care
External advisers	Jeremy Nolan – Head of Internal Audit Tony Stanley – DHSC Internal Audit George Smiles - External Audit - National Audit Office (NAO) Jill Hearne – National Audit Office (NAO)
Observers	Dafni Moschidou, Department of Health and Social Care (DHSC)
Staff in attendance	Peter Thompson, Chief Executive Morounke Akingbola, Head of Finance Richard Sydee, Director of Finance and Resources Paula Robinson, Head of Planning and Governance Helen Crutcher, Risk and Business Planning Manager David Crook, R2 Project Manager Dan Howard, Chief Information Officer Andrew Leonard, Senior Inspector Debbie Okutubo, Governance Manager

1. Welcome and declarations of interests

1.1 The Chair welcomed everyone present and requested that all attendees introduced themselves.

1.2 There were no declarations of interest.

2. Minutes of the meeting held on 4 December 2018

2.1 The minutes of the meeting held on 4 December 2018 were agreed as a true record of the meeting and approved for signature by the Chair.

3. Matters arising

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

3.2 Members asked that in future there should be more notice if training scheduled for a meeting day was cancelled.

3.3 Margaret Gilmore stated that she was unable to attend the AGC meeting scheduled for 18 June 2019.

4. Regulatory and Register management

4.1 The Chief Information Officer and one of the senior inspectors spoke to the presentation. It was noted that staffing changes were concluding within the Information and IT team, in response to one of the team's operational risks, and that all necessary steps were being taken to mitigate the risk. Mitigations also included a shift away from over-reliance on individuals with particular knowledge, an increased emphasis on the use of external experts when necessary.

4.2 The biggest strategic risk was cyber security, but continual improvements meant that there were effective mitigations in place.

4.3 In response to questions, it was noted that there were opportunities to drive improvements in the sector through proportionate regulation and working with centres.

4.4 It was explained that centres were encouraged to use their quality management systems to best effect, rather than rely solely on being inspected. Also, that it was the norm for NHS funded centres to have, at the very least part-time quality managers. However non-compliances would still arise between inspections owing to factors like staff turnover, NHS resources and new legislation.

4.5 Members discussed various aspects of the inspection regime and suggested that regulatory changes could lead to non-compliance in some instances as centres' awareness of new responsibilities may vary and urged inspectors to be aware of this.

4.6 It was noted that not all centres held certificates to import.

4.7 The external auditor suggested that work on the inspection methodology was in the developmental stage and would be modified as matters progressed.

4.8 Members heard that a refresh of the Choose a Fertility Clinic (CaFC) information has not taken place during the development of PRISM, and that this meant that the CaFC data had not been refreshed for three years. This would be remedied later in the year. AGC agreed that they should be kept informed of progress on this.

Action

4.9 Discussion at a future Authority workshop on whether licenses could be issued for 5 years for centres that have a strong history of compliance, rather than 4 years. Interim inspections of such centres could also possibly be lighter touch.

4.10 Capacity and resilience issues should continue to be captured in the risk register and kept under review.

4.11 AGC to be kept informed about the planned refresh of CaFC data later this year.

5. Finance and resources update

5.1 The Director of Finance and Resources gave a verbal update. The annual budget and predicted income would be taken to the Authority meeting on 13 March for approval. There was growth in income of 6.9%. There was a surplus in the expenditure budget which would be discussed with Department of Health and Social Care (DHSC). Consideration would be given to reducing the HFEA's reserves, either by proposing particular projects of benefit to patients, or by not drawing down Grant in Aid payments from the Department.

5.2 The biggest risk in 2019/20 was in relation to the civil service pension and the planned 6.1% increase to the employer contribution rate. Government guidance was still awaited, but this was likely to have an impact in 2020.

5.3 The winding down of the PRISM project would release some budget during the coming financial year.

6. Resilience, Business Continuity Management and Cyber Security

6.1 Team risks included recent turnover in two posts. Regarding the shared service between HFEA and HTA, consideration would be given to reconfiguring or merging the two finance teams after the next office move, since the two organisations would then be co-located. The estates work would be an important main focus going forward.

6.2 The Chief Information Officer gave an update on IT infrastructure and development support.

6.3 The committee requested a comparative analysis against the last report presented to them and asked that it come back to the June 2019 AGC Meeting.

6.4 The business continuity plan was also discussed, and AGC noted that a test of the business continuity system was being planned. It was agreed that a report would also be presented to the June 2019 meeting. The Chief information Officer and a member agreed to discuss business continuity after the meeting.

Action

6.5 Chief Information Officer to bring both items to June meeting.

7. Internal Audit

a) 2019/20 audit plan

7.1 The Head of Internal Audit confirmed that the internal audit plan had been discussed with the Senior Management Team (SMT). Members noted that the plan appeared to be the right risk-based approach.

7.2 In response to a question about the planned audit of governance arrangements, the Internal Auditor explained that some items appeared on the plan on a regular cyclical basis, and that the HFEA's governance was last audited in 2013/14.

7.3 In response to a question, it was noted that the IT estate and cyber security had been considered, but it was agreed that it would not be on the plan for the coming year. However, records management was included.

7.4 The AGC confirmed that they were content with the draft 2019/20 internal audit plan.

b) Progress report

7.5 The Internal audit team continue to work with HFEA to resolve all outstanding recommendations from previous audit reviews. Regular communication was in place to ensure that appropriate action was being taken to implement all recommendations.

7.6 In response to a question, the Internal Auditor reported that the Anti Fraud and GDPR audits were completed but were too late to be brought to the March meeting. Also, the Business Continuity follow-

up audit was not presented, because the documentation was not received in time for submission with the March papers. It would therefore be presented at the June 2019 Meeting.

8. Implementation of audit recommendations

8.1 The Head of Finance reported that there were fourteen outstanding audit recommendations, of which four remained open.

8.2 The committee was advised that there were two further audits – GDPR and anti-fraud, not included in the tracker.

8.3 The committee discussed the possible future appointment of a non-executive member to AGC who had a background in technology. It was noted that this had been discussed after the last meeting, during the annual review of effective governance. This could now be taken off the tracker as it could be deemed complete.

8.4 AGC noted that the movement of one team member from the PRISM team to the Inspectorate had been delayed pending completion of the PRISM project and data migration. This will remain on the tracker as the Chief Information Officer and Chief Inspector continue to review the impact. The plan was for the staff member to move across by Spring 2019.

9. External audit – interim feedback

9.1 The External Auditor gave a verbal update. It was noted that the National Audit Office (NAO) were midway through the interim audit and that there were no major issues detected. An update would be provided in due course.

9.2 During the discussion, it was noted that the NAO was changing its way of testing and had returned to substantive testing, for audit efficiency purposes. This was still being developed, with no major impact this year. The timetable would remain the same, unless changes due to EU exit had an impact. Comptroller and Auditor General sign-off would remain as before.

10. Draft governance statement

10.1 The draft governance statement was presented by the Director of Finance and Resources. It was noted that this was produced in draft form for the committee to have the opportunity to input into it at this early stage. The statement would include how risk would be addressed and assurance given.

10.2 It was suggested that given the variety and complexity of the risks we face, the overall appetite for risk was low. It was agreed, in accordance with earlier risk appetite discussions, that our appetite (or tolerance) for risk could vary, in that the HFEA may sometimes take strategic risks in order to pursue its strategic ambitions.

10.3 The management of operational risks gave assurance that statutory functions were managed appropriately and mitigated against proportionately. Teams continued to maintain a risk log capturing their own operational risks and shared with the Corporate Management Group (CMG).

This bottom up approach meant that the management of risk remained embedded in the organisation.

10.4 It was noted that the statement was still in draft form and would be quality checked before the final version was published.

Action:

10.5 The committee requested that the legal requirements for HFEA needed to be clearly laid out in the governance statement and that a list of some of the cutting-edge things achieved during the last year could be added to it. The current political climate should also feature in the statement, including the management of the consequences of EU exit. Additional information could also be considered about information management and security, and the GDPR.

10.6 The committee recommended rewording the first sentence on risk appetite.

11. General Data Protection Regulation update

11.1 The Director of Finance and Resources reported that the Digital Projects Migration was still outstanding. Information held on Registers was exempt, but work had been undertaken to identify the information that did fall within the scope of GDPR.

11.2 It was reported that in the last year there were no data losses.

12. Digital Programme update

12.1 The Chief Executive introduced this item. He noted that PRISM development, development of APIs and engagement with the sector were going well.

12.2 The Chief Information Officer provided an update. He noted that data migration continued to present a challenge due to complexities surrounding the EggBatchID linkage.

12.3 To facilitate a discussion with AGC, five options were presented. These would continue to be assessed and a more detailed assessment would be available in early April.

12.4 Part of the further discussion would involve looking at the level of risk and cost implications along with business impact, also the communication with clinics, which would be very important.

12.5 In response to a question, members were advised that the totality of our income could not be exceeded. Any usage of reserves would require prior sign-off from the DHSC.

12.6 Committee members noted that staffing levels in teams would need to be evaluated rather than consider external people/resources as some options were suggesting.

12.7 Following discussion, members felt that option two was the most feasible. However, it would be important to fully understand the parameters, the timetable and the resource requirements.

12.8 The Chair suggested that all options should remain on the table until further discussion had been held.

12.9 It was believed that trying to run two Registers would be counter-productive as it could create and increase inherent risks.

Action:

12.10 The five options to be assessed and a detailed analysis circulated to members in April 2019 and a teleconferencing meeting could be arranged.

12.11 It would be discussed at Authority and the Chief Executive would consider the depth of the information to be discussed in an open meeting.

12.12 A date would be arranged imminently. Information would be circulated nearer the time of the meeting, to ensure information provided was as up to date as possible.

13. EU exit

13.1 The Chief Executive discussed the timeline and current possible scenarios with the Committee. He further stated that two principal risks were currently being managed: the legal risk and the operational risk in the event of a no deal EU exit.

13.2 There were five pieces of EU law relevant to HFEA responsibilities and all had been transposed into domestic UK law. Even though it did not appear that there were significant legal or regulatory risks, it was believed that there could be considerable consequential work, including revisions to the Code of Practice and General Directions, (and therefore our process for approving special directions for import and export).

13.3 HFEA readiness had been assessed and it was well placed to manage required changes

14. Estates

14.1 The Director of Finance and Resources reported that the London Estates Programme (LEP) had a deadline of November 2020, but at present no firm decision had been made about the HFEA's future office location. Contract negotiation was in progress.

14.2 A business case was expected to be signed off at the end of March, with further clarity for ALBs in April or May. A project group had been started up to consider what the HFEA's needs were, in advance of agreeing the full logistical details of a move. Further updates would be provided at future meetings.

15. Strategic risk register

15.1 The Risk and Business Planning Manager presented the Strategic Risk Register and noted that points made in the meeting under other items would be incorporated into the risk register after the meeting. The emerging risk on employer pension contributions would be incorporated into the finance risk once this was clearer. Also, aspects of the work on PRISM would be added to the risks on cyber security and regulatory effectiveness.

15.2 The committee noted that SMT reviewed the register on 28 January 2019 and had reviewed all risks, controls and scores.

15.3 The committee particularly discussed the capability risk. The process of appointing a replacement for the Director of Compliance was ongoing but posed a risk meanwhile. The recent absence of the Chief Inspector on sick leave had increased the level of risk. In response to a question, it was noted that the Chief Executive was currently line managing the director department, but the arrangement was not sustainable in the long term. The interim solution may be to consider a secondment, until a permanent replacement would be in post.

15.4 Meanwhile, senior inspectors were working hard to manage the team and activities in this area were going well.

Action:

15.5 Comments on risk from this and other agenda items to be incorporated into the risk register.

16. AGC forward plan

16.1 The Head of Finance presented the AGC forward workplan.

16.2 The Anti-Fraud, Bribery and Corruption Policy and the Public Interest Disclosure (Whistleblowing) Policy would be presented at committee on an annual basis.

16.3 The committee noted the forward workplan.

Action:

16.4 Items above to be added to the forward plan.

17. Whistle blowing and fraud policies

17.1 The counter fraud, bribery and corruption policy had been implemented to ensure people working for the HFEA are aware that fraud can exist and how to respond if fraud was suspected.

17.2 It was highlighted that staff had to have regard to related policies and procedures including:

a. HFEA Standing Financial Instructions and Financial Procedures

b. HFEA Staff Handbook

c. Disciplinary and Whistleblowing Policies.

17.3 The whistle blowing policy applied to all employees, both permanent and fixed term.

17.4 Members noted that it was important that when it came to internal disclosure, staff felt comfortable with who they were reporting to, which was not necessarily always the line manager.

17.5 Also, that the Chair of the Authority should be another person that staff could report to.

17.6 At related meetings with staff, it was agreed that there should be a note taker or witness in addition to the staff member.

Action:

17.7 Above suggested amendments to be incorporated into the whistle blowing policy.

18. Contracts and procurement

18.1 The Head of Finance gave the committee an update on existing contracts. It was noted that since the last meeting, no new contract had been signed off.

19. Any other business

19.1 The Chief Executive agreed to circulate the staff survey to members with a short report.

19.2 Two Audit and Governance committee members had attended a conference for non-executives, facilitated by the National Audit Office (NAO) and gave feedback to the meeting.

19.3 The Chair thanked the team and members present and extended her appreciation to those who had worked on the reports but did not attend the meeting.

19.4 Members and auditors retired for their confidential session.

19.5 The next meeting will be held on Tuesday,18 June 2019 at 10am.

20. Chair's signature

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

Signature

Name

Anita Bharucha

Date

18 June 2019

Audit and Governance

Committee meeting minutes

Strategic delivery:	☐ Setting standards	☐ Increasing and informing choice	☐ Demonstrating efficiency economy and value
Details:			
Meeting	Special Audit and Governance Committee		
Agenda item	3		
Paper number	AGC (18/06/2019) 671		
Meeting date	18 June 2019		
Author	Debbie Okutubo, Governance Manager		
Output:			
For information or decision?	For decision		
Recommendation	Members are asked to confirm the minutes as a true and accurate record of the meeting		
Resource implications			
Implementation date			
Communication(s)			
Organisational risk	☒ Low	☐ Medium	☐ High
Annexes			

Minutes of Audit and Governance Committee (AGC) meeting held on 8 May 2019

Church House, Deans Yard Westminster, London, SW1P 3NZ

Members present	Anita Bharucha (Chair) Margaret Gilmore Mark McLaughlin – via teleconferencing Geoffrey Podger
Apologies	None
Observers	None
Staff in attendance	Peter Thompson, Chief Executive Richard Sydee, Director of Finance & Resources Clare Ettinghausen, Director of Strategy & Corporate Affairs Dan Howard, Chief Information Officer David Crook, R2 Programme Manager Debbie Okutubo, Governance Manager

1. Welcome and declarations of interests

1.1 The Chair welcomed everyone present and explained the reason why the special Audit and Governance committee meeting had to be convened.

1.2 There were no declarations of interest.

2. Data Migration: Options review

2.1 In March 2019 AGC received an update on data migration, system development, the implementation of the new register and associated transitional activities.

2.2 Options ranged from using existing in-house resource (option 1), using a third party provider (option 2), using a team of internal staff to manually resolve (options 3 and 5). Option 4 was using current data only and leaving historic data in the old register.

2.3 At the March meeting, there was a request that all five options be explored in depth, and that they be assessed against business, financial and reputational risks. Also, the impact and consequence on patients, individuals and the sector and that it be brought back to the committee.

2.4 To ensure information provided was as up to date, this extraordinary meeting was arranged, with a report circulated beforehand as previously agreed. The paper appraised the options and assessed against the criteria above. It set out a recommendation, including costs and timeline for data migration, and the subsequent launch of PRISM.

2.5 AGC members noted that options 3, 4 and 5 would require the maintenance of two registers, could create a significant number of errors and/or require a high level of manual checking which would therefore create substantial risk in relation to sensitive patent data. For that reason, members agreed that discussion should focus on options 1 and 2. Members noted that the paper

by the Executive recommended Option 2 and invited the Executive to set out the advantages and risks of this option, compared with option 1, in more detail.

2.6 Officers responded that Option 1

- Was heavily reliant on a single individual's expertise
- The staff member currently covering it was using methodology that could be improved on

2.7 On the other hand, Option 2 had the added value of

- Bringing in extra technical resource who could assist at the granular level of the process
- Additional technical support to speed up the work
- Mitigating the risk of depending on a single person
- Having an improved governance framework around the work

2.8 In response to a question, it was noted that data structures in the old Register were structurally different to the new Register. Data in the old Register was not linked (i.e. cycles were not linked over time) and data in the old Register was stored in forms each with multiple treatments.

2.9 With regards to the November 2019 deadline, members were given the assurance that

- Contingency had been built into the timeframe
- The track record of the company proposed was that it is not likely that they will miss the deadline set
- There was a financial incentive to finish on time and a penalty if they did not.

2.10 The committee were advised that part of the ongoing work was to transfer and share knowledge with other team members prior to procurement of the expert company.

2.11 It was noted that option 2 could deliver all of the programme benefits being sought, but not until EggBatchID had been resolved, supported by a third party consultancy company experienced in complex data migrations.

2.12 Choose a Fertility Clinic (CaFC) would also be updated with refreshed data as planned later in 2019. This was important as the data is out of date.

2.13 This option would also improve resilience through the use of specialists, have an improved technological solution and it would support PRISM go-live in November 2019.

2.14 At go-live there would be a full set of verified data with minimal disruption to clinics. It would reduce the delay and disruptions to existing processes, reduce the reliance on a single developer, and reduce the need for a programme manager and data migration specialist for an extended period.

2.15 Members sought clarification on the legal procurement position including the reason for not publishing a tender.

2.16 Following clarification, the Director of Finance sent a note to AGC members explaining that our procurement policy is aligned with wider CCS, Cabinet Office and DHSC procurement guidance. Non-compliance was permissible but SMT approval was required to be sought for a single tender waiver (STW). However, in order not to fall foul, the reasons for not complying must generally fall in to one of two categories. HFEA relied on the latter category which was that the expertise required was only available from one source. SMT's recommendation was therefore to proceed to engage with the agreed provider to undertake the work plan discussed at the 8 May 2019 AGC discussion.

2.17 Members were advised that the option 2 proposal was broadly affordable although it would use all available contingency, and re-prioritising may need to happen. The Chair asked for this to be drawn to the attention of Authority members at the meeting which followed immediately after AGC.

2.18 In response to a question, it was noted that the cost of the organisational move scheduled for Autumn 2020 would be met by the DHSC. The IT was mainly 'cloud based' which minimised financial implications of moving and re-platforming on-premise hardware.

Decision

2.19 Members agreed Option 2 (use of third party provider) as it was believed that it would bring in additional assurance over completion of the programme, deliver the programme benefits sought quickly and avoid the current and future disbenefits associated with the other options. It provided a level of certainty for programme completion not available in other options.

2.20 AGC members advised Officers to explore the financial implications at the next accountability meeting with the DHSC.

2.21 Members to receive further correspondence in relation to the procurement decision not to tender.

2.22 The Chief Executive would be writing to PRs and clinics, as part of the preparation for go-live.

2.23 AGC will be sent a copy of the letter for information.

2.24 Officers confirmed that they would forward monthly updates to AGC on programme progress and outstanding work.

3. Chair's signature

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

Signature

Name

Anita Bharucha

Date

18 June 2019

Matters Arising from previous AGC

Strategic delivery:	☐ Safe, ethical, effective treatment	☐ Consistent outcomes and support	☐ Improving standards through intelligence
Details:			
Meeting	Audit and Governance Committee		
Agenda item	4		
Paper number	AGC (18/06/2019) 672 MA		
Meeting date	18 June 2019		
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	Ongoing		
Communication(s)			
Organisational risk	☐ Low	☒ Medium	☐ High

Numerically:

- 7 items added from October 2018 meeting, 6 ongoing
- 4 items carried over from earlier meetings, 3 ongoing
- Items removed: 12.4 (12/6/18), 5.5, 11.6, 12.5, 13.6 (9/10/18)

ACTION	RESPONSIBILITY	DUE DATE	PROGRESS TO DATE
Matters Arising from the Audit and Governance Committee – actions from 12 June 2018 meeting			
9.10 The Committee to receive monthly updates highlighting any variances and increased risk.	Chief Information Officer		**Update** - on the three identified risks and issues concerning data migration, additional development work and loss of key staff to be given in the meeting
9.11-9.12 There would be joint approval between the Committee and key staff for data migration sign off, with full assurance being provided concerning the move of the Any further significant issues would be addressed through a meeting with the Committee Chair and key staff. Register to the Microsoft Azure 'cloud'.	Chief Information Officer		**Update** – This item has been superseded as options paper was submitted for Committee approval in March 2019.
Matters Arising from the Audit and Governance Committee – actions from 9 October 2018 meeting			
3.8 The Committee Secretary to contact members regarding availability for training after the meeting on 4 December 2018 or 5 March 2019	Committee Secretary		**Update** – Training to take place in the autumn
8.13 The Committee to receive a further paper on the digital programme, which would be followed-up by a teleconference, prior to the launch of PRISM, to attain approval to proceed.	Chief Information Officer		**Update** – this item relates to 9.11 from the June 2018 meeting and was coved in paper presented. Committee has since met and agreed options paper presented. Contingency funds to be used to action option 2.

Matters Arising from the Audit and Governance Committee – actions from 5 March 2019 meeting			
4.9 Discussion at future Authority workshop on whether licences could be issued for 5 years for centres with a good compliance record			**Update –** a suggestion for future Authority meetings.
4.10 Capacity and resilience issues to be captured on the Strategic Risk Register and kept under review	Risk and Business Planning Manager		**Update –** This has been done.
4.11 Authority to be kept informed about planned refresh of CaFC data later this year	Chief Information Officer		**Update** – on the agenda under Digital Project update.
6.5 Comparative analysis report on IT infrastructure and development support and report on Business Continuity test	Chief Information Officer		**Update –** on the agenda under Resilience, Business Continutity Management and Cyber Security
10.5 Clearly lay out legal requirement for HFEA in annual governance statement and list cutting-edge things achieved during the year. Current political climate and consequences of EU exit to be included.	Director of Finance and Resources		**Update –** we have made reference to not being an risk-averse regulator. Due to the sensitivity of EU exit, we have avoided making any reference to this in the AGS. We would need clearance from DHSC Coms if we do.
12.10-21.12 Five options and detailed analysis to be circulated in April. Discussion to take place at Authority	Chief Information Office		**Update** – paper has been presented and decision made.

15.5 Comments on risks discussed under other agenda items to be incorporated into the Strategic Risk Register	Risk and Business Planning Manager		**Update** – appropriate amendments have been made.
16.4 Add the Anti-Fraud, Bribery and Corruption Policy and the Whistleblowing Policy to forward plan to ensure presented annually.	Head of Finance		**Update** – Added to forward plan. There is work being undertaken that will affect both policies. Policies to be re-published/shared with staff by July.
17.7 Amendments suggested by the committee to be made to the Whistleblowing policy.	Head of Finance		**Update -** policy amended with suggestions from Committee.

Human Resources update 2019

Strategic delivery:	☒ Safe, ethical, effective treatment	☒ Consistent outcomes and support	☒ Improving standards through intelligence
Details:	**Human Resources Update June 2019**		
Meeting	Audit and Governance Committee meeting		
Agenda item	9		
Paper number	AGC (18/06/2019) 678 YA		
Meeting date	18 June 2019		
Author	Yvonne Akinmodun, Head of Human Resources Peter Thompson, Chief Executive		
Output:			
	For Information		
Recommendation	The Committee is asked to note and comment on the: a. executive response to staff opinion (section 2) b. work underway on developing new metrics to better measure and manage organisational resilience (turnover) (section 3) c. work on options for a new pay and grading framework (section 4)		
Organisational risk	☐ Low	☒ Medium	☐ High

1. Introduction

1.1. The staff in any organisation are central to its continued success. That is why we are committed to providing regular updates to the AGC on a range of HR matters. We last discussed HR issues with the AGC in December 2018, where we focussed on organisational capability, notably through the lens of staff turnover. This paper responds to that discussion and also provides a broader overview, focussing on staff opinion, turnover, and work that is underway on a potential new pay and grading system designed to enable clearer and easier development.

2. Staff survey

2.1. In recent years we have measured staff opinion through an annual survey. The survey is based on the civil service survey, which covers 15 aspects of employee engagement. The civil service staff survey also has the advantage of providing us with a benchmark, in terms of how we measure against the civil service average. And for several years HFEA staff scores were significantly better than the civil service average in most areas.

2.2. That picture changed in 2017. The staff survey conducted in November 2017 showed a significant downturn in several aspects of engagement, largely in response to the high level of uncertainty caused by the organisational restructure carried out earlier that year. We attempted to address this downturn in a variety of ways, including a refreshed HR Strategy. The most recent staff survey conducted in 2018 did not, however, result in survey scores returning to their previous level. The top themes with the highest and lowest score are shown below.

Top 5 highest scoring areas were:

- My work
- Organisations purpose
- My manager
- Organisational culture – I am trusted to do my work
- Resources and workload

Top 5 low scoring areas were:

- Pay and benefits
- Leadership and change
- Learning and development
- Harassment and bullying
- Your plans for the future – How long do you plan to remain at the HFEA

2.3. The survey also provides an open text option for staff to respond on an issue of their choice. The key themes that emerged from the responses in 2018 included:

- A feeling that our current pay structures are not fair
- Concerns over the effectiveness of our IT resources
- A sense that SMT and the Authority are too disconnected from day to day business
- Concerns about the fairness of our performance management system
- Concerns about aspects of our current office space

2.4. In December 2018, we held an all staff meeting to review some of the themes from the survey and identify actions to address them. The key actions we have put in place include:

- Monthly open Q&A sessions with a member SMT
- The publication of actions from SMT and CMG meetings on the staff intranet
- An extended range of learning and development provision
- A quarterly pulse survey to review a select number of themes identified as needing improvement.

2.5. In March 2019, we conducted the first of a quarterly pulse survey which focused on 4 aspects of employee engagement: teams, my manager, staff perception of SMT and learning and development.

The results from the pulse survey indicated:

- Perception of senior management has improved – an increase of 20%
- Staff continue to feel supported by their line managers
- However, 4 respondents still reported bullying and harassment – 4 too many
- And on learning and development 11% more feel they have access to the right opportunities compared with previous years but concerns about career progression remain.

2.6. We will conduct a second pulse survey in July, using themes from the main survey to see what effect the actions taken so far have had.

3. Staff turnover

3.1. As AGC know, staff turnover has been high for some time now. Over the last 12 months turnover has stood at 27%. While some degree of turnover is a good thing, turnover at this level is difficult to manage; it creates knowledge gaps and additional workload on the staff that remain. At AGC in December 2018 we provided an overview of the information we held on turnover, largely drawn from exit interviews conducted by the HR team. Those interviews revealed that the top 3 reasons given by staff for leaving were:

- Pay
- Lack of opportunity for progression
- Poor relationship with line manager/ or senior managers

3.2. We believe that we now need to develop a more sophisticated set of metrics for measuring and planning for turnover. While we can do relatively little about pay and progression in the short to

medium term, we can gain a better understanding of the likely numbers of staff who might move in the future.

3.3. The length of service of staff who left the HFEA in the last 12 months shows that the average length of time staff remained with the HFEA was 4.25 years. Breaking those figures down further, we can see that staff in more junior roles (band 2 and some at band 3) were more likely to move on after around 2 years of joining the organisation. Whereas staff in managerial roles at band 3 and above tended to remain with the organisation for longer – 4 years or more.

3.4. Looking ahead, we will use this data to model the likely vulnerability of different grades or teams in the organisation**.**

4. Pay and grading

4.1. In order to maintain the operational effectiveness of the HFEA we must recruit high-quality staff and look to retain the staff we have for longer. Both of these goals require that we retain competitive levels of pay. As a result of the pay restraint in the public sector, the HFEA has not revised the band minimum for its pay bands since 2010. This has led to difficulties recruiting in to some office-based vacancies, with IT and Governance roles proving particularly difficult to fill through normal recruitment channels.

4.2. Our recruitment difficulties will be further exacerbated by the fact that the other aligned public sector pay scales (most notably the new NHS Agenda for Change (AfC) pay bands) are pulling ahead of our existing bands and this will likely contribute to staff churn if we fail to keep pace with the wider public sector.

4.3. For other roles, however, employment with the HFEA remains attractive, particularly those roles where remote working is possible which has allowed us to recruit people from a wider geographic pool. Remote working also provides some existing staff with a more attractive work/life balance. Our current experience is that many staff are keen to take the opportunity of more remote working, but that not all posts are suitable for a predominantly home-based workforce. This then raises issues of equity of the pay framework for those who are required to be office-based relative to those who are able to work remotely and who do not incur commuting costs and time.

4.4. In March this year, SMT put forward a paper to the Remuneration Committee (RemCo) setting out the first draft of a proposed new pay and grading system. The review concluded that most of our roles were at about the right pay point and the relatively 'flat' grading structure was defensible, though there was a case for creating more opportunities for progression in parts of the organisation. RemCo were broadly supportive but asked for more detail on one or two points.

4.5. However, any new pay and grading system would also need the approval of the DHSC and, given the continuing position of the public finances, any new proposal for the HFEA would have to be self-funding. Moreover, the timing of the submission of any business case will have to await the publication of the Treasury's annual guidance on pay within the public sector. The planned office move in 2020 will also provide an opportunity to look again at the balance between home and office-based working in the organisation.

5. Recommendations

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

Digital Programme Update: June 2019

Strategic delivery:	☒ Setting standards	☐ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item	11		
Paper number	AGC (18/06/2019) 680 DH		
Meeting date	18 June 2019		
Author	Dan Howard, Chief Information Officer		
Output:			
For information or decision?	For information		
Recommendation	The Committee is asked to note: • Progress made on development of PRISM, release of APIs, and supplier / clinic engagement; • The detailed update on progress surrounding data migration; • The update plan for the refresh of Choose a Fertility Clinic data; and, • The financial update		
Resource implications	Within budget		
Implementation date	During 2019 - 20		
Communication(s)	Regular, range of mechanisms		
Organisational risk	☐ Low	☒ Medium	☐ High
Annexes:	None		

1. Background and summary

1.1. This paper provides an update on progress relating to system development, data migration, the implementation of the new register and the associated transitional activities.

1.2. Recently provided papers have set out options for resolution of the EggBatchID issue and subsequent PRISM go-live. In light of the detail provided in previous updates this paper is a summary of progress.

1.3. Development of APIs will be complete in June and PRISM will be completed in July. We will release a beta version of PRISM to the sector for evaluation and feedback in August.

1.4. Following AGC approval, we have commissioned the third party data migration company to support resolution of the EggBatchID issue. Work is underway and a progress update is below.

1.5. The Register team is readying itself to support a Choose a Fertility Clinic data refresh in October with detailed data validation taking place with clinics over the summer. An outline of our approach is below.

1.6. As the work progresses, we will continue to provide regular updates to AGC on progress.

2. PRISM and APIs

2.1. PRISM and API development are almost complete. Change of role, validation and an update to the application 'look and feel' is now complete. Production environment testing has been completed (with some subsequent changes to be made). API user guides have been documented and API testing has continued. 'Gamete sources' is nearing completion. This combined with previous development work means that around 95% of PRISM is now complete.

2.2. We will launch the second iteration of the APIs on 14 June. PRISM will be complete shortly afterwards between 22 and 31 July 2019. Following release of the beta system it is likely that a small number of minor updates (to include validation rules, look and feel, and labelling work) will take place ahead of the full launch later this year.

2.3. Once the system is complete, continued system testing will take place and the user guide will be completed. We will launch a beta version of PRISM to the sector in August, to capture feedback and support clinics' familiarisation with the new system. This will be ahead of a full PRISM launch at the end of November, once data migration has concluded.

3. Data Migration

3.1. In May, AGC reviewed five data migration options and subsequently provided authorisation for option 2; to work with a data migration specialist (Iergo) to accelerate the resolution of EggBatchID linkages. The order has been placed and this work is in progress.

3.2. Iergo are working to a methodology called Practical Data Migration, recognised by the British Computer Society. It covers the full data migration lifecycle from gap analysis, through migration design and execution and includes decommissioning of legacy databases and retirement of systems. Their approach includes additional technical

resource. These elements combined will help ensure that the agreed timescales for EggBatchID resolution are met.

3.3. Within the business engagement stream Iergo will focus on the key deliverables needed to switch off and decommission the existing register once the new register has been tested, loaded with data and 'cut-over' to the new register.

3.4. We will carefully monitor progress on resolution of the EggBatchID linkages and compare this to the acceptable threshold, in terms of clinic impact and business risk, to allow a considered, measured and successful data migration. This means that it will not be necessary to wait until we have reached a data quality level of 100%, and we will recommend 'cut-over' when the business risk and the impact is forecasted to be at a manageable and acceptable level.

3.5. AGC will be requested to provide final approval in early October to support a go-live at the end of November. The final approval will review agreed business risk elements and specific data migration elements. The data migration elements will include: migration audit, training, testing, data retention, and go-live restrictions, clinic user experience, fall-back, fallout, review of business items and business processes.

3.6. We have agreed a weekly reporting cycle with Iergo and the Digital Programme Board will continue to receive monthly updates.

4. Choose a Fertility Clinic (CaFC) update

4.1. The register team is readying itself to support a CaFC refresh over the summer. Refreshing CaFC clinic performance data requires extensive data validation by clinics.

4.2. We are keen to support the sector and give them ample time to undertake necessary checks and have extended our usual validation window from around 6 weeks to almost three months.

4.3. We will be producing and circulating validation reports later in June covering:

- Pregnancy rates per cycle and birth rates: January 2015 until December 2018
- 3-year aggregated pregnancy rates per cycle and live birth rates per cycle: January 2015 until December 2017
- Pregnancy rates per cycle only: January 2017 until December 2017

4.4. The register team will be on hand to provide support, guidance and the CaFC refresh will take place in October 2019.

5. Clinic and sector engagement

5.1. We continue to respond to clinic queries during PRISM, API development, and the CaFC refresh and we continue to provide regular updates to the sector and system suppliers.

5.2. No significant issues have been raised to date.

6. Financial

6.1. We continue to closely monitor our financial position against our agreed capital and revenue budget.

6.2. In April / May 2019 we have spent £101,000 (comprising £26,000 capital and £75,000 revenue), with £225,000 (revenue) remaining this financial year. No further capital is required.

6.3. The capital element of £26,000 is within our £100,000 capital allocation and the revenue is being managed with the operational constraints we have, both known and forecasted.

7. Recommendation

The Committee is asked to note:

- Progress made on development of PRISM, release of APIs, and supplier / clinic engagement;
- The update on progress surrounding data migration;
- The update plan for the refresh of Choose a Fertility Clinic data; and,
- The financial update

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 (18/06/2019) 681 DH		
Meeting date	18 June 2019		
Author	Dan Howard, Chief Information Officer		
Output:			
For information or decision?	For information		
Recommendation	The Committee is asked to note: • The contract award relating to the procurement to secure a supplier for essential IT infrastructure and development support; • The results of business continuity plan test undertaken in March 2019; and, • The update on work to upgrade our telephone system, network and video-conferencing facilities		
Resource implications	Within budget		
Implementation date	Ongoing		
Communication(s)	Regular, range of mechanisms		
Organisational risk	☐ Low	☒ Medium	☐ High
Annexes:	None		

1. Introduction and background

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

1.2. In March 2019 AGC received an update on our IT infrastructure and IT development support arrangements. We signalled an intention to secure a longer term support arrangement in 2019. The associated procurement work has concluded and the contract has been awarded. An update is below.

1.3. Our Business Continuity arrangements were tested in March 2019 and the results are below.

1.4. AGC have regularly received details on our plan to make improvements to our telephone system and video-conferencing facilities. An update is below.

2. IT infrastructure support

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

2.2. A review identified a requirement for first and second line support for several key areas such as user account management, support for Microsoft Virtual Machine and Azure servers, management of specialist databases, website management, support for specialist systems such as our licensing system. Our inhouse team will continue to concentrate on supporting HFEA-specific systems and the HFEA-specific configuration of enterprise systems. The requirement included development support to work with a future small in-house team to maintain the software code relating to in-house applications. We tendered for a 2 year plus 2 year contract term providing expected stability for a four year period.

2.3. We issued a tender using Crown Commercial Services framework RM3745, lot 8, providing a total of around 200 days of support per year. Most of the 200 days will be for infrastructure support rather than development support, although we do have the ability to flex this as necessary.

2.4. We received one bid in response to that tender, from the incumbent supplier, Alscient. Given the single bid we considered our options and the reason for the low response rate. We concluded that was due to the low value of the contract, in comparison to other published tenders. We also agreed it was necessary that we used a CCS framework given the contractual assurances that gives us (for example - security standards, operational standards, external checks).

2.5. The single bid was evaluated by the panel, and scores moderated. In the absence of other bids to assess it against, the panel assessed the price element against framework day rates and on that basis the panel felt that the proposal offered good value for money.

2.6. The bid met the quality and price threshold we had set (no answer was scored below the acceptable score), the score awarded was 75.5%, and the contract was awarded earlier this month.

3. Business Continuity test

Approach

3.1. We undertook a business continuity test in March 2019 and this section sets out the results and lessons learnt.

3.2. Before the test took place, we completed several actions which included tasks such as making sure we have up to date mobile numbers for staff, updated out of hours building arrangements for IT access, reviewing IT disaster recovery documents, and circulating updated business continuity plan guidance documentation for staff on the Intranet.

3.3. The test took place on Thursday 21 March at 18.18. It involved sending out two automated text messages to staff mobile phones, one to let people know that it was a BCP test with the BCP site link, and a second with some guidance on how to log on and what to do when they have logged on.

3.4. While we did not send the text message to Authority Members, we invited feedback from Authority Members the following day and specifically sought advice before the test from Margaret Gilmore, who has Cyber Security responsibility.

3.5. After the test we monitored the site to monitor the access rate. We provided additional guidance afterwards to staff who were not able to access it at the time.

Results

3.6. Over 40% of eligible staff accessed the site within the first 4 hours. By Friday morning, over 60% had accessed the BC site. Over the next 7 days, a total of 49 out of 65 staff had logged on.

3.7. Feedback was very positive with very few people reporting technical difficulties. We noted that there was a significant improvement in 'ease of access' for staff when comparing against previous tests. We have concluded this was due to increased awareness and better internet browsers on mobile devices.

3.8. A reminder was sent out on 26 March to the 25 people who had not yet logged on at that point.

3.9. A review took place on 26 March and a range of lessons learnt / actions were noted and agreed. They include amending our internal processes for the test, refining how we contact Authority Members, and improving ongoing awareness.

3.10. On 15 April 10 people had not logged on and support was given to those unable to log on.

3.11. Our Corporate Management Group were updated on progress and considered the results of the test at its meeting on 17 April 2019 and all staff received an update following the test via the Intranet.

3.12. Specialist BCP training will be reviewed for those with a role in delivering business continuity plans, and this will be delivered by August 2019

3.13. Our BCP policy was subsequently reviewed and updated in May 2019 to reflect lessons learned during this test, the frequency at which the document should be updated, the frequency of testing, and how the HFEA would respond to a disruptive incident should our offices be closed for a prolonged period.

3.14. We will continue to monitor our business continuity arrangements in line with the actual or perceived risk.

4. Telephone system and video conferencing upgrades

4.1. In March 2019 AGC received an update on our work to improve our telephony system, network and associated infrastructure. This upgrade will deliver significant benefits: providing the network capacity we require, supporting improvements to video-conferencing, aligning to our 'cloud first' IT strategy and enabling a smooth transition to new premises in 2020.

4.2. A test range of telephone numbers were ported into the new service and the server improvements - moving the Skype for Business server from on-premise to cloud data-centre have been completed. The bandwidth improvements (from 100Mb/second to 200Mb/second) were successfully implemented in June 2019 involving downtime of less than one hour.

4.3. Detailed testing with five migrated Skype users was carried out and feedback was very positive; call quality, video quality and document sharing functioned as expected and user feedback was good.

4.4. Now that testing is complete we will transition all users into the new service, review effectiveness and capture feedback. The timing of this was delayed so as not to coincide with the electronic document management system upgrade (which took place in May / June 2019) and is now dependant on getting an external supplier to surrender the HFEA number ranges to a new supplier. While this has proved challenging, it is expected that the change will be completed before the end of July 2019.

4.5. Once complete, and where appropriate, we will look to use the new facilities for HFEA committee meetings. While the new teleconference facilities will facilitate a 'good' service within HFEA, external factors may influence the quality of the user experience. External factors include WiFi or 3G/4G strength, network connection speed, firewall rules on an external corporate network, and software installed or speed of the connecting device. We will issue guidance to Members as part of the rollout to committees.

5. Recommendation

The Committee is asked to note:

- The contract award relating to the procurement to secure a supplier for essential IT infrastructure and development support;
- The results of business continuity plan testing; and,
- The update on work to upgrade our telephone system, network and video-conferencing facilities

Strategic risk register

Strategic delivery:	☒ Safe, ethical, effective treatment	☒ Consistent outcomes and support	☒ Improving standards through intelligence
Details:			
Meeting	Audit and Governance Committee		
Agenda item	13		
Paper number	AGC (18/06/2019) 682 HC		
Meeting date	18 June 2019		
Author	Helen Crutcher, Risk and Business Planning Manager		
Output:			
For information or decision?	For information and comment		
Recommendation	AGC is asked to note the latest edition of the risk register, set out in the annex.		
Resource implications	In budget.		
Implementation date	Strategic risk register and operational risk monitoring: ongoing. SMT review the strategic risk register monthly. AGC reviews the strategic risk register at every meeting. The Authority reviews the strategic risk register periodically (at least twice per year).		
Communication(s)	Feedback from AGC will inform the next SMT review in June.		
Organisational risk	☐ Low	☒ Medium	☐ High
Annexes	Annex 1: Strategic risk register		

1. Latest reviews

1.1. Authority received the risk register at its meeting on 8 May and SMT reviewed the register at its meeting on 20 May. SMT reviewed all risks, controls and scores.

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

1.3. One of the six risks is above tolerance.

2. Recommendation

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

Latest review date – 20/05/2019

Strategic risk register 2018/19

Risk summary: high to low residual risks

Risk area	Strategy link*	Residual risk	Status	Trend**
C1: Capability	Generic risk – whole strategy	**12 – High**	At tolerance	⇔⇔⇔⇔
RE1: Regulatory effectiveness	Improving standards through intelligence	**9– Medium**	Above tolerance	⇧⇔⇔⇔
CS1: Cyber security	Generic risk – whole strategy	**9 – Medium**	At tolerance	⇔⇔⇔⇔
FV1: Financial viability	Generic risk – whole strategy	**9 – Medium**	At tolerance	⇔⇔⇔⇧
LC1: Legal challenge	Generic risk – whole strategy	**8 – Medium**	Below tolerance	⇔⇔⇔⇔
ME1: Effective communications	Safe, ethical effective treatment Consistent outcomes and support	**6 – Medium**	At tolerance	⇔⇔⇔⇔

* Strategic objectives 2017-2020:

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

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

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

Consistent outcomes and support: Improve access to treatment

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

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

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

Recent review points are: SMT 18 March 2019 ⇨ SMT 15 April 2019⇨ Authority 8 May 2019 ⇨ SMT 20 May

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

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

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

Commentary
Below tolerance. While planning our 2019/20 budget, we took a prudent approach, utilising our predictive model, planning based on 2% growth on the current budget rather than against the recent trend, which is higher. This should ensure that should we see a drop in treatment volumes, the HFEA will be able to meet its financial commitments from its annual receipts. Increases of 6% have been confirmed to the civil service pension employer contributions, of which we must fund 2.5% within the HFEA budget with the remainder centrally funded. This was budgeted for and does not pose a particular risk to financial viability. The delays in completing the data migration element of the digital projects has increased costs in 2019/20. In May 2019 the Audit and Governance Committee agreed to secure specialist data migration support to complete this work. This must come out of existing budgets and so will have a knock-on effect on other planned work. To ensure that we do not exceed our control totals with DHSC we now need to reprioritise expenditure in other areas of the organisation. The score of the Regulatory effectiveness risk was adjusted to reflect the possible impact of these risk sources in March.

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

Our monthly income can vary significantly as: • it is linked directly to level of treatment activity in licensed establishments • we rely on our data submission system to notify us of billable cycles.	Our reserves policy takes account of monthly fluctuations in treatment activity and we have sufficient cash reserves to function normally for a period of two months if there was a steep drop-off in activity. The reserves policy was reviewed by AGC in December 2018. If clinics were not able to submit data and could not be invoiced for more than three months we would invoice them on historic treatment volumes and reconcile this against actual volumes once the submission issue was resolved and data could be submitted.	Ongoing – Richard Sydee In place – Richard Sydee
Annual budget setting process lacks information from directorates on variable/additional activity that will impact on planned spend.	Annual budgets are agreed in detail between Finance and Directorates with all planning assumptions noted. Quarterly meetings with Directorates flag any shortfall or further funding requirements. All project business cases are approved through CMG, so any financial consequences of approving work are discussed.	Quarterly meetings (on-going) – Morounke Akingbola Ongoing – Richard Sydee
Additional funds are needed for the completion of the data migration work and this will constrain HFEA finances and affect other planned and ad hoc work.	The most cost-effective approach will be 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. Where possible, costs will be covered by the IT budget, reducing the impact on key delivery teams and other strategic deliverables. First quarter budgets will be reviewed at CMG, and this will allow us to consider the impact and reprioritise as appropriate.	Procurement underway – Richard Sydee Ongoing – Richard Sydee July CMG meeting – Richard Sydee
Inadequate decision-making leads to incorrect financial forecasting and insufficient budget.	Within the finance team there are a series of formalised checks and reviews, including root and branch analyses of financial models and calculations. The organisation plans effectively to ensure enough time and senior resource for assessing core budget assumptions and subsequent decision making.	In place and ongoing - Richard Sydee Quarterly meetings (on-going) – Morounke Akingbola
Project scope creep leads to increases in costs beyond the levels that have been approved.	Finance staff present at Programme Board. Periodic review of actual and budgeted spend by Digital Projects Board (formerly IfQ) and monthly budget meetings with finance. Any exceptions to tolerances are discussed at Programme Board and escalated to CMG at monthly meetings, or sooner, via SMT, if the impact is significant or time-critical.	Ongoing – Richard Sydee or Morounke Akingbola Monthly (on-going) – Olaide Kazeem

Failure to comply with Treasury and DHSC spending controls and finance policies and guidance leads to serious reputational risk and a loss of financial autonomy or goodwill for securing future funding.	The oversight and understanding of the finance team ensures that we do not inadvertently break any rules. The team's professional development is ongoing, and this includes engaging and networking with the wider government finance community. All HFEA finance policies and guidance are compliant with wider government rules. Policies are reviewed annually, or before this if required. Internal oversight of expenditure and approvals provides further assurance (see above mitigations).	Continuous - Richard Sydee Annually and as required – Morounke Akingbola
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
DHSC: Legal costs materially exceed annual budget because of unforeseen litigation.	Use of reserves, up to contingency level available. The final contingency for all our financial risks would be to seek additional cash and/or funding from the Department.	Monthly – Morounke Akingbola
DHSC: GIA funding could be reduced due to changes in Government/policy.	A good relationship with DHSC Sponsors, who are well informed about our work and our funding model.	Accountability quarterly meetings (on-going) – Richard Sydee
	Annual budget has been agreed with DHSC Finance team. GIA funding has been provisionally agreed through to 2020.	December/January annually, – Richard Sydee

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

Inherent risk level:			Residual risk level:		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	4	16 – High	**4**	**3**	**12- High**
Tolerance threshold:					**12 - High**

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

Commentary

At tolerance.

This risk and the controls are focused on business as usual capability, rather than capacity, though there are obviously some linkages between capability and capacity. Since we are a small organisation, with little intrinsic resilience, it seems prudent to retain a low tolerance level.

For 18/19 turnover was 26.8%. Evidence suggests that the two main drivers of high turnover are the continuing constraints on public sector pay and the relatively few development opportunities in small organisations like the HFEA. In response, we have revised our recruitment strategy using a wider range of national and social media and recruitment agencies to improve the number and quality of applicants. This approach is having some success and we have in recent months attracted several high-quality candidates. We are also taking active steps to improve retention focussing on things that we can control like learning and development.

Following the 2018 staff survey and the December 2018 staff awayday, an action plan has been shared with staff and this is being reviewed on a regular basis to ensure that progress continues. As part of this, in April 2019 we ran the first of several more frequent, shorter surveys to get a sense of the concerns of staff at regular intervals. Work has taken place to improve the organisational learning and development offer, with several courses planned throughout the first quarter of 2019/20 to target training needs identified by staff and the corporate management group.

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

Causes / sources	Mitigations	Timescale / owner

High turnover, sick leave etc., leading to temporary knowledge loss and capability gaps.	Organisational knowledge captured via documentation, handovers and induction notes, and manager engagement. We have developed corporate guidance for all staff for handovers. A checklist for handovers is circulated to managers when staff hand in their notice. This checklist will reduce the risk of variable handover provision.	In place – Yvonne Akinmodun Checklist in use – Yvonne Akinmodun
	Vacancies are addressed speedily, and any needed changes to ways of working or backfill arrangements receive immediate attention. CMG and managers prioritise work appropriately when workload peaks arise.	In place – Yvonne Akinmodun In place – Peter Thompson
The vacant Director of Compliance and Information is being covered by other staff, this creates a risk that key pieces of work are unable to be delivered due to resource pressures and unforeseen capability gaps.	The successful candidate pulled out two weeks before she was due to start. A new search is underway and active consideration is being given to additional interim support arrangements. Other staff are covering elements of this role and work is being re-prioritised as required.	Underway – Peter Thompson
Poor morale could lead to decreased effectiveness and performance failures.	Communication between managers and staff at regular team and one-to-one meetings allows any morale issues to be identified early and provides an opportunity to determine actions to be taken. The new intranet, which launched in October 2018 has enabled more regular internal communications.	In place, ongoing – Peter Thompson In place – Jo Triggs
	Work continues to implement actions in the people plan which launched in April 2018 and reflected staff feedback. Further actions have been identified through the 2018 staff survey and awayday. An action plan is in place from January 2019 and is being regularly reviewed to ensure that actions are effective. In 2018 new benefit options were implemented, including PerkBox and a buying and selling of annual leave policy (launched July 2018).	Annual survey and staff conferences – Yvonne Akinmodun In place - Peter Thompson
Increased workload either because work takes longer than expected or reactive diversions arise.	Careful planning and prioritisation of both business plan work and business flow through our Committees. Regular oversight by CMG – standing item on planning and resources at monthly meetings.	In place – Paula Robinson
	Oversight of projects by both the monthly Programme Board and CMG meetings, to ensure that projects end through due process (or closed, if necessary). We are re-launching our interdependencies matrix, which supports the early identification of	In place – Paula Robinson Matrix relaunching early 2019/20 –

	interdependencies in projects and other work, to allow for effective planning of resources.	Paula Robinson
	Learning from Agile methodology to ensure we always have a clear 'definition of done' in place, and that we record when products/outputs have met the 'done' criteria and are deemed complete.	Partially in place – further work to be done in 2019/20 - Paula Robinson
	Team-level service delivery planning for the next business year, with active involvement of team members. CMG will continue to review planning and delivery. Requirement for this to be in place for each business year.	In place – Paula Robinson
	Planning and prioritising data submission project delivery, and therefore strategy delivery, within our limited resources.	In place until project ends – Dan Howard
Future increase in capacity and capability needed to process and assess licensing activity including mitochondrial donation applications. Since Summer 2017, we have experienced resource pressures relating to the Statutory Approvals Committee, caused in part by mitochondrial donation applications and also the increasing complexity and volume of PGD conditions.	Licensing processes for mitochondrial donation are in place (decision trees etc). An external review of the HFEA licensing processes was carried out to assess current capabilities and processes and make changes for the future. We are in the process of implementing the relevant proposals. To mitigate the present capacity and capability issues, the executive has signed up more experienced mitochondria peer reviewers, have received feedback on the process and have made administrative changes to improve it. This includes improvements to the application form, to prevent additional administration and/or unnecessary adjournments. In February 2019, we increased staffing capacity in the licensing team to address the capacity and capability issues. This enables us to accommodate our existing level of demand, increasing our capacity to support the licensing function as we handle more business and ensure our committees are supported effectively.	Licensing review implementation underway from September 2018 – Paula Robinson / Clare Ettinghausen
We may not be able to find time to implement the People Plan to maximise organisational capability given our small organisational capacity and ongoing delivery of business as usual.	Small focus groups and all staff awaydays have been utilised to make the most of staff time and involve wider staff in developing proposals. The next all staff awayday is in July.	Ongoing – Yvonne Akinmodun

A number of staff are simultaneously new in post. This carries a higher than normal risk of internal incidents and timeline slippages while people learn and teams adapt.	Recognition that a settling in period where staff are inducted and learn, and teams develop new ways of working is necessary. Formal training and development are provided where required. Knowledge management via records management and documentation and the HR team has revised onboarding methods to make them clearer and more effective.	In progress – Peter Thompson In place – Yvonne Akinmodun
The future office move, occurring in 2020, may not meet the needs of staff (for instance location), meaning staff decide to leave sooner than this, leading to a significant spike in turnover, resulting in capability gaps.	We will consult with staff, to ensure that their needs are taken into account, where possible, when planning for the move. We plan to explore possible knowledge and capability benefits arising from the office move, such as the potential to open up closer working and career progression with other health regulators.	Early engagement with staff and other organisations underway and ongoing – Richard Sydee
The new organisational model may not achieve the desired benefits for organisational capability Delay in completing our digital projects means that elements of the new model have not been fully implemented. It will therefore take more time for us to validate whether the changes have been effective.	The model will be kept under review following implementation to ensure it yields the intended benefits. The staff survey provided an opportunity for staff to reflect on whether change has been well managed. The results will help to inform any further actions related to the model.	A review of the new model was presented to AGC in June 2018. Staff survey in October 2018 – Peter Thompson
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
Government/DHSC: The government may implement further cuts across all ALBs, resulting in further staffing reductions. This would lead to the HFEA having to reduce its workload in some way.	We were proactive in reducing headcount and other costs to minimal levels over a number of years. We have also been reviewed extensively in the past eg, the Triennial Review in 2016.	In place – Peter Thompson
Government/DHSC The UK leaving the EU may have unexpected operational consequences for the HFEA which divert resource and threaten our ability to deliver our strategic aims.	The department has provided guidance about the impact of a no-deal EU exit on the import of gametes and embryos. We continue to work closely to ensure that we are prepared and can provide detailed guidance to the sector at the earliest opportunity, to limit any impact on patients. We have provided ongoing updates to the sector. In December 2018, we commenced an EU exit project to ensure that we fully consider implications and are able to build enough knowledge and capability to handle the effects of the UK's exit from the EU, as a third country in relation to import and export of gametes. This project includes our role in communicating with the sector on the effects of EU	Communications ongoing – Peter Thompson

	exit, to ensure that clinics are adequately prepared in terms of staffing and access to equipment and materials. We have continued to engage with the DHSC and clinics to prepare for a 'no deal' scenario. As of early April 2019 immediate 'no deal' plans have been stepped down by the DHSC and we have informed clinics accordingly.	

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

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
5	4	20 – Very high	**3**	**3**	**9 - Medium**
Tolerance threshold:					**9 - Medium**

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

Commentary
Above tolerance. We have undertaken further cyber security (penetration) testing of the new digital systems such as PRISM and the Register, to ensure that these remain secure. The results have not revealed any significant issues. The third and final test is scheduled ahead of go-live. Go-live has been delayed owing to issues with data migration. Options were considered by AGC in May and revised deployment plans are being developed. The delay poses no increased cyber risk. We continue to assess and review the level of national cyber security risk and take action as necessary to ensure our security controls are robust and are working effectively. The results of a cyber security audit were received in in December 2018, the rating of this audit was moderate with no significant weaknesses found.

Causes / sources	Mitigations	Timescale / owner
Insufficient governance or board oversight of cyber security risks (relating to awareness of exposure, capability and resource, independent review and testing, incident preparedness, external linkages to learn from others).	AGC receives reports at each meeting on cyber-security and associated internal audit reports. The Vice Chair of the Authority is regularly appraised on actual and perceived cyber risks. Internal audit report on data loss (October 2017) gave a 'moderate' rating, recommendations have been actioned, one final recommendation is being reported at each AGC meeting. A further cyber security internal audit report was finalised in December 2018. A final report on cyber security will be signed off by AGC before any decision is made to go live with PRISM.	Ongoing regular reporting – Director of Compliance and Information/ Dan Howard Ongoing – Dan Howard Deployment date of project to be confirmed once ongoing

		data migration issue resolved – 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.	The website and Clinic Portal are secure and we have been assured of this. The focus now is on obtaining similar assurance through penetration testing report to the SIRO in relation to the remaining data submission deliverables (PRISM). The second of three rounds of penetration testing has been completed and there have been no significant issues found so far.	Penetration testing underway throughout development and ongoing – Peter Thompson/ Dan Howard
There is a risk that IT demand could outstrip supply meaning IT support doesn't meet the business requirements of the organisation and so we cannot identify or resolve problems in a timely fashion. We do not currently have a developer in post.	We continually refine the IT support functional model in line with industry standards (ie, ITIL). We undertook an assessment of our ticketing systems and launched a new system in November 2018. Following implementation, we will introduce ways to capture user feedback and this functionally will be introduced in May 2019. Our vision is to have an internal team working in partnership with a third-party software development provider. The tender for the third-party contract (Infrastructure support and Development support) has concluded and we awarded the contract in May. The service is based on the ITIL framework (IT service standard). Our strategy was to recruit to the in-house software development team following a workload review. This has been completed and once the contract for ongoing support has begun we will begin the recruitment process.	Approved per the ongoing business plan – Dan Howard Tender process completed to procure a longer-term support arrangement – Dan Howard Recruitment to internal development team underway from June 2019 – Dan Howard
Confidentiality breach of Register or other sensitive data by HFEA staff.	Staff are made aware on induction of the legal requirements relating to Register data. All staff have annual compulsory security training to guard against breaches of confidentiality although we are now due to refresh this. Updated information risk training has been identified and staff are expected to complete this during April / May 2019. Relevant and current policies to support staff in ensuring high standards of information security. There are secure working arrangements for all staff both in the office and when working at home (end to end data encryption via the internet, hardware encryption)	In place – Peter Thompson A review of current IT policies is ongoing – Dan Howard

	Further to these mitigations, any malicious actions would be a criminal act.	
There is a risk that technical or system weaknesses lead to loss of, or inability to access, sensitive data, including the Register.	Back-ups of the data held in the warehouse in place to minimise the risk of data loss. Regular monitoring takes place to ensure our data backup regime and controls are effective. We are ensuring that a thorough investigation takes place prior, during, and after moving the Register to the Cloud. This involves the use of third party experts to design and implement the configuration of new architecture, with security and reliability factors considered.	In place – Dan Howard Results of penetration testing have been positive. The new Register will be deployed once ongoing data migration issue is resolved, date TBC – Dan Howard
Business continuity issue (whether caused by cyber-attack, internal malicious damage to infrastructure or an event affecting access to Spring Gardens).	Business continuity plan and staff site in place. The BCP information cascade system was tested in March 2019 and CMG reviewed the plan and agreed revisions in May. Existing controls are through secure off-site back-ups via third party supplier. A cloud backup environment has been set up to provide a further secure point of recovery for data which would be held by the organisation. The cloud backup environment for the new Register has been successfully tested. Once the final penetration tests are complete we will utilise this functionality as we go live with our new Register and submission system.	BCP in place, regularly tested and reviewed – Director of Compliance & Information/ Dan Howard Undertaken monthly – Dan Howard The new Register cloud backup environment will be deployed once ongoing data migration issue is resolved – date TBC – Dan Howard
The corporate records management system (TRIM) is unsupported and unstable and we are carrying an increased risk of it failing. The organisation may be at risk of poor records management until the new system is functioning and records successfully transferred.	A formal project to replace our electronic document management system is underway, for delivery of a new system in May 2019. We are continuing to manage the existing risk with the TRIM system by minimising changes and monitoring performance regularly. All staff have been reminded to continue to use TRIM to ensure records are complete.	A new system, Content manager, was introduced in May 2019 and is now being bedded in – Dan Howard

Cloud-related risks.	Detailed controls set out in 2017 internal audit report on this area. We have in place remote access for users, appropriate security controls, supply chain security measures, appropriate terms and conditions with Microsoft Azure, Microsoft ISO 27018 certification for cloud privacy, GCloud certification compliance by Azure, a permission matrix and password policy, a web configuration limiting the service to 20 requests at any one time, good physical and logical security in Azure, good back-up options for SQL databases on Azure, and other measures.	In place – Dan Howard
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
None. Cyber-security is an 'in-common' risk across the Department and its ALBs.		

LC1: There is a risk that the HFEA is legally challenged given the ethically contested and legally complex issues it regulates.

Inherent risk level:			**Residual risk level:**		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	5	20 – Very high	**2**	**4**	**8 - Medium**
Tolerance threshold:					**12 - High**

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

Commentary
Below tolerance. We accept that in a contested area of public policy, the HFEA and its decision-making will be legally challenged. Legal challenge poses two key threats: • that resources are substantially diverted • that the HFEA's reputation is negatively impacted by our participation in litigation. These may each affect our ability to regulate effectively and deliver our strategy. Both the likelihood and impact of legal challenge may be reduced, but it cannot be avoided entirely. For these reasons, our tolerance for legal risk is high. We have not had any active legal action since October 2018.

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

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

	The Compliance team stay in close communication with the Head of Legal to ensure that it is clear if legal involvement is required, to allow for effective planning of work. The Compliance management team monitor the number and complexity of management reviews to ensure that the Head of Legal is only involved as appropriate.	In place – Sharon Fensome Rimmer, Director of Compliance & Information
Moving to a bolder strategic stance, eg, on add-ons or value for money, could result in claims that we are adversely affecting some clinics' business model or acting beyond our powers. Any changes could be perceived as a threat – not necessarily ultimately resulting in legal action, but still entailing diversion of effort.	Risks considered whenever a new approach or policy is being developed. Business impact target assessments carried out whenever a regulatory change is likely to have a significant cost consequence for clinics. Stakeholder involvement and communications in place to ensure that clinics can feed in views before decisions are taken, and that there is awareness and buy-in in advance of any changes. Major changes are consulted on widely.	In place – Clare Ettinghausen
The Courts approach matters on a case by case basis and therefore outcomes can't always be predicted. So, the extent of costs and other resource demands resulting from a case can't necessarily be anticipated.	Scenario planning is undertaken with input from legal advisors at the start of any legal challenge. This allows the HFEA to anticipate a range of different potential outcomes and plan resources accordingly.	In place – Peter Thompson
Legal proceedings can be lengthy, and resource draining and divert the in-house legal function (and potentially other colleagues) away from business as usual.	Panel in place, as above, enabling us to outsource some elements of the work.	In place – Peter Thompson
	Internal mechanisms (such as the Corporate Management Group, CMG) in place to reprioritise workload should this become necessary.	In place – Peter Thompson
HFEA process failings could create or contribute to legal challenges, or weaken cases that are otherwise sound,	Licensing SOPs were improved and updated in Q1 2018/19, committee decision trees in place. Advice sought through the Licensing review on specific legal points, so that improvements can be identified and implemented. A project to implement these is underway.	In place – Paula Robinson From October 2018 – Paula Robinson
	Up to date compliance and enforcement policy and related procedures to ensure that the Compliance team acts consistently according to agreed processes.	In place but in the process of being reviewed – Catherine Drennan
Legal parenthood consent cases are ongoing, and some are the result of more recent failures (the mistakes occurred	The Head of Legal continues to keep all new cases under review, highlighting any new or unresolved compliance issues so that the	In progress and ongoing – Catherine Drennan,

within the last year). This may give rise to questions about the adequacy of our response when legal parenthood first emerged as a problem in the sector (in 2015).	Compliance team can resolve these with the clinic(s).	Sharon Fensome-Rimmer, Director of Compliance & Information
Storage consent failings at clinics are leading to a significant diversion of legal resource and additional costs for external legal advice.	We have taken advice from a leading barrister on the possible options for a standard approach for similar cases. We are in the process of considering how the advice can be interpreted in guidance which can be applied broadly across the sector. Significant amendments to guidance in the Code of Practice dealing with consent to storage and extension of storage. This guidance will support clinics to be clearer about their statutory responsibilities and thus prevent issues arising in the future. Additional support is planned at the Annual Conference and through the revision of the PR entry Programme (PREP) in the autumn.	Done in Q1 2018/19 – Catherine Drennan Revised version of the Code launched January 2019 – Laura Riley
GDPR requirements require a large number of changes to practice. If we fail to comply with the requirements, this could open the HFEA up to legal challenge and possible fines from the Information Commissioner's Office.	The GDPR project introduced a number of new and updated policies and processes, to ensure that the HFEA complies with the requirements. These will now be bedded into BAU to ensure that they are effective. The project was handled proactively, with a joint HFEA and HTA project team and sponsored directly by the Director of Finance and Resources to ensure senior oversight. Although the project was closed in October, ongoing actions are being closely monitored to ensure effective compliance. AGC have regular updates on progress.	Ongoing-Richard Sydee
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
DHSC: HFEA could face unexpected high legal costs or damages which it could not fund.	If this risk was to become an issue then discussion with the Department of Health and Social Care would need to take place regarding possible cover for any extraordinary costs, since it is not possible for the HFEA to insure itself against such an eventuality, and not reasonable for the HFEA's small budget to include a large legal contingency. This is therefore an accepted, rather than mitigated risk. It is also an interdependent risk because DHSC would be involved in resolving it.	In place – Peter Thompson
DHSC: Legislative interdependency.	Our regular communications channels with the Department would ensure we were aware of any planned change at the earliest stage. Joint working arrangements would then be put in place as needed, depending on the scale of the change. If	In place – Peter Thompson

	necessary, this would include agreeing any associated implementation budget. The Department are aware of the complexity of our Act and the fact that aspects of it are open to interpretation, sometimes leading to challenge. Sign-off for key documents such as the Code of Practice in place	

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

Inherent risk level:			Residual risk level:		
Likelihood	Impact	Inherent risk	**Likelihood**	**Impact**	**Residual risk**
4	4	16 - High	**3**	**3**	**9 – Medium**
Tolerance threshold:					**6 - Medium**

Risk area	Risk owner	Links to which strategic objectives?	Trend
Regulatory effective-ness RE 1: Inability to translate data into quality	Peter Thompson, Chief Executive (pending start of new Director of Compliance & Information)	Improving standards through intelligence: use our data and feedback from patients to provide a sharper focus in our regulatory work and improve the information we produce	⇧⇔⇔⇔

Commentary
Above tolerance. Data submission work continues although delivery has been somewhat delayed as described under risks above. We have experienced difficulties with migrating Register data and this has delayed the launch of PRISM and the new Register. Fully developed data migration options went to AGC in May and a plan for deployment was agreed which will involve extending the delivery timeframes. These issues obviously cause a delay to accessing improved data and we consequently raised this risk in March 2019.

Causes / sources	Mitigations	Timescale / owner
IfQ has taken longer than planned, and there will be some ongoing development work needed leading to delays in accessing the benefits.	Data Submission development work is now largely complete, however decisions related to data migration must be taken before clinic implementation is possible. Oversight and prioritisation of remaining development work will be through the IT development programme board with oversight from AGC.	Deployment date of data submission project to be confirmed once ongoing data migration issue resolved – Director of Compliance & Information
Risks associated with data migration to new structure,	Migration of the Register is highly complex. IfQ programme groundwork focused on current state of Register. There is substantial high-level	Deployment date to be confirmed

compromises record accuracy and data integrity.	oversight including an agreed migration strategy which is being followed. The migration will not go ahead until agreed data quality thresholds are met. AGC will have final sign off on the migration.	once ongoing data migration issue resolved, with regular reporting on progress prior to this – Director of Compliance & Information /Dan Howard
We could later discover a barrier to meeting a new reporting need, or find that an unanticipated level of accuracy is required, involving data or fields which we do not currently focus on or deem critical for accuracy.	IfQ planning work incorporated consideration of fields and reporting needs were agreed. Decisions about the required data quality for each field were 'future proofed' as much as possible, through engagement with stakeholders to anticipate future needs and build these into the design. Further scoping work would occur periodically to review whether any additions were needed. The structure of the new Register makes adding additional fields more straightforward than at present.	In place regular reviews to occur once the Register goes live – Director of Compliance & Information
Risk that existing infrastructure systems – (eg, Register, EDI, network, backups) which will be used to access the improved data and intelligence are unreliable.	Maintenance of desktop, network, backups, etc. core part of IT business as usual delivery. In March 2018 CMG agreed to a new approach, including some outsourcing of technical second and third line support, this provides greater resilience against unforeseen issues or incidents. As noted above under CS1, we have a further temporary arrangement in place for ongoing external support for 4/5 months from November 2018 and are in the process of tendering for ongoing support.	In place – Dan Howard
Insufficient capability and capacity in the Compliance team to enable them to act promptly in response to the additional data that will be available.	Largely experienced inspection team. The inspection team is now at complement although there will be a bedding in period for newer staff.	In place – Director of Compliance & Information
Failure to integrate the new data and intelligence systems into Compliance activities due to cultural silos.	Work has been undertaken to bed in systems, such as the patient feedback mechanism, and this is now a part of Compliance business as usual.	Ongoing - Yvonne Akinmodun
Regulatory monitoring may be disrupted if Electronic Patient Record System (EPRS) providers are not able to submit data to the new Register	Earlier agreements to extend part of 'IfQ' delivery help to address this risk by extending the release date for the data submission project. Plan in place to deal with any inability to supply data.	Ongoing - Director of Compliance & Information

structure until their software has been updated.	The Compliance management team will manage any centres with EPRS systems who are not ready to provide Register data in the required timeframe. Centres will be expected to use the HFEA's PRISM if they are unable to comply. Early engagement with EPRS providers means the risk of non-compliance is slim.	
Data migration efforts are being privileged over data quality leading to an increase in outstanding errors	The Register team uses a triage system to deal with clinic queries systematically, addressing the most critical errors first.	In place – Director of Compliance & Information
	We undertake an audit programme to check information provision and accuracy.	In place – Director of Compliance & Information
Excessive demand on systems and over-reliance on a few key expert individuals – request overload – leading to errors	PQs and FOIs have dedicated expert staff to deal with them although they are very reliant on a small number of individuals. We have systems for checking consistency of answers.	In place – Clare Ettinghausen
	There is a dedicated team for responding to OTRs and all processes are documented to ensure information is provided consistently	In place – Dan Howard
Risk interdependencies (ALBs / DHSC)	**Control arrangements**	**Owner**
None	-	-

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

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

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

Commentary
At tolerance. Authority discussed our communications strategy in January 2019 and agreed that good progress had been made. Communications should be derived from the strategy and aligned with the key organisational objectives. This included the approach to building relationships with political and other stakeholders and developing a wider public affairs approach. Conversations about messaging and engagement are central to early discussion about the new 2020-2023 strategy to ensure that we take a joined-up approach that takes full advantage of our channels and a public affairs approach.

Causes / sources	Mitigations	Timescale / owner
Some of our strategy relies on persuading clinics to do things better. This is harder to put across effectively, or to achieve firm outcomes from.	When there are messages that need to be conveyed to clinics through the inspection team, staff work with the team so that a co-ordinated approach is achieved and messages that go out to the sector through other channels (eg clinic focus) are reinforced. When there are new or important issues or risks that may impact patient safety, alerts are produced collaboratively by the Inspection, Policy and Communications teams.	In place - Sharon Fensome-Rimmer, Laura Riley, and Jo Triggs
Patients and other stakeholders do not receive the correct guidance or information.	Communications strategy in place, including social media and other channels as well as making full use of our new website. Stakeholder meetings with	In place and reviewed periodically

	the sector in place to help us to underline key campaign messages. Our new publications use HFEA data more fully and makes this more accessible. Policy team ensures guidance is created with appropriate stakeholder engagement and is developed and implemented carefully to ensure it is correct. Ongoing user testing and feedback on information on the website allows us to properly understand user needs. We have internal processes in place which meet The Information Standard. Procurement of new providers for the Donor Conceived Register undertaken and successful. The executive is facilitating interim arrangements to ensure that there is a smooth transition of the service to the new supplier and effective information and support continues to be in place for donor conceived people.	(last review occurred Jan 2019) – Jo Triggs Ongoing – Nora Cook-O'Dowd In place – Laura Riley, Jo Triggs In place –Jo Triggs Certification in place, although the assessment and certification scheme is being phased out – Jo Triggs Contract awarded and transition arrangements in place – Dan Howard
We are not able to reach the right people with the right message at the right time.	We have an ongoing partnership with NHS.UK to get information to patients early in their fertility journey and signpost them to HFEA guidance and information. Planning for campaigns and projects includes consideration of communications channels. When developing policies, we ensure that we have strong communication plans in place to reach the appropriate stakeholders. Extended use of social media to get to the right audiences. The communications team analyse the effectiveness of our communications channels at Digital Communications Board meetings, to ensure that they continue to meet our user needs.	In place – Jo Triggs In place and ongoing – Jo Triggs In place - Laura Riley, Jo Triggs In place– Jo Triggs Ongoing – Jo Triggs
Risk that incorrect information is provided in PQs, OTRs or FOIs and this may lead to misinformation and misunderstanding by patients, journalists and others.	PQs and FOIs have dedicated expert staff to manage them and additional staff are being trained to ensure there is not over-reliance on individuals. We have systems for checking consistency of answers and a member of SMT must sign off every PQ response before submission.	In place - Clare Ettinghausen Clare Ettinghausen /SMT - In place

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

Reviews and revisions

SMT review – May 2019 (20/05/2019)

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

- C1 – SMT discussed changes relating to the Director of Compliance and Information post which would now need to be recruited to again. They noted that further controls were being considered to ensure that there was continued support in place for staff while we managed this ongoing vacancy.
- FV1 – SMT discussed the financial viability risk at length. SMT reflected on the impact of recent decisions taken by AGC about the solution for completing the delayed data migration. Further funds were required for this and this would therefore affect the cash available to undertake other work. SMT reflected this meant that the inherent likelihood of having insufficient resource had increased, as had the residual risk level and adjusted the score accordingly. The impact on key regulatory and strategic work will be carefully managed through reprioritisation and SMT did not feel that the impact level of this particular risk had raised such that the score should be revised.
- SMT noted that a first draft for a new office move strategic risk would be developed with the Director of Finance and Resources over the coming weeks and this would be discussed with SMT in June.

Authority review – May 2019 (08/05/2019)

Authority reviewed all risks, controls and scores and made the following point:

- The Chair of AGC noted that given the conversations with AGC that morning (at an exceptional meeting), about the data migration progress and costs to complete this, the financial viability risk should

be reviewed, to reflect the impact of the agreed additional spend and resulting constraints on HFEA finances.

SMT review – April 2019 (15/04/2019)

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

- RE1 – SMT discussed the changes relating to the delay to data migration delivery. Discussions would be occurring with AGC in May.
- C1 – SMT discussed the progress made in recruiting to the licensing function and reflected this in the register.

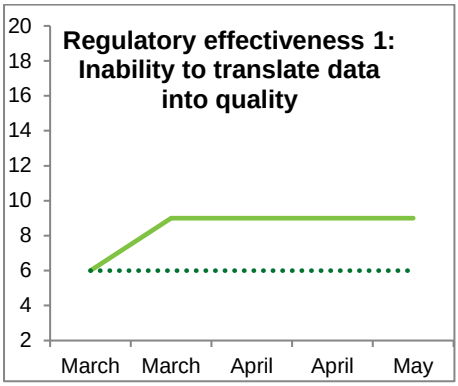
SMT review – March 2019 (18/03/2019)

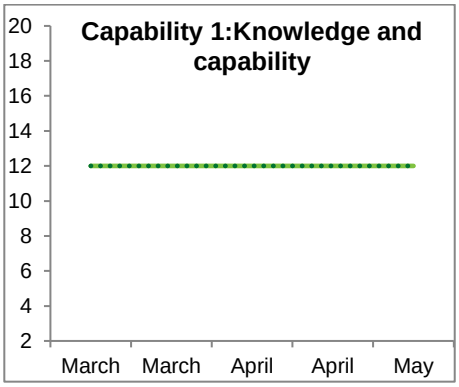
SMT reviewed all risks, commentary, controls and scores and made the following detailed points:

- FV1 –SMT discussed the impact of increased pensions contributions on the budget and agreed that this did not materially impact the level of this risk or affect financial viability. SMT reflected that there was uncertainty as to the costs of completing the data migration, however work would be reprioritised as necessary to ensure that we did not exceed control totals.
- C1 – SMT agreed to an additional risk area being included, reflecting the particular risk related to the vacant Director of Compliance post. This was being proactively managed and did not increase the overall risk score.
- CS1 RE1 – SMT discussed the impact of the digital projects delays and noted that all timeframes should be updated. The primary implication was on the RE1 risk, since this was about taking advantage of improved systems. SMT agreed to raise the risk score from six to an above tolerance score of nine. The risks were being proactively managed as part of discussions on the options for data migration, which would be considered by AGC.
- SMT discussed when the right time would be to expand on the estates/office move risk and agreed this this could be added as a separate risk area in this register once the scoping of the internal project had progressed and the business case agreed.

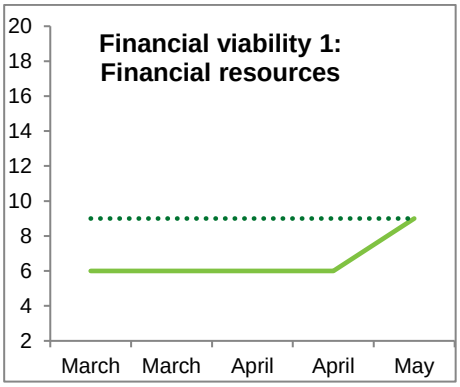
Risk trend graphs

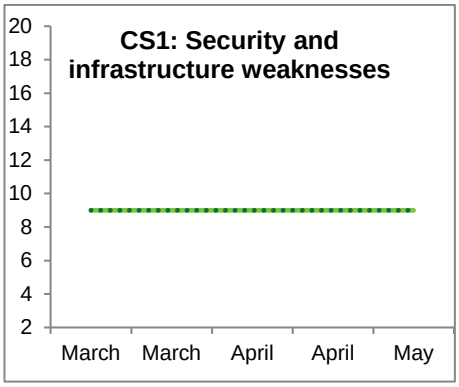
High and above tolerance risks

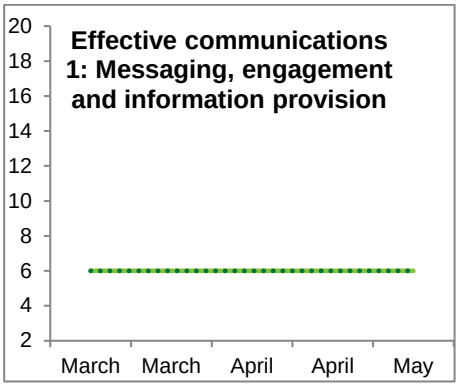


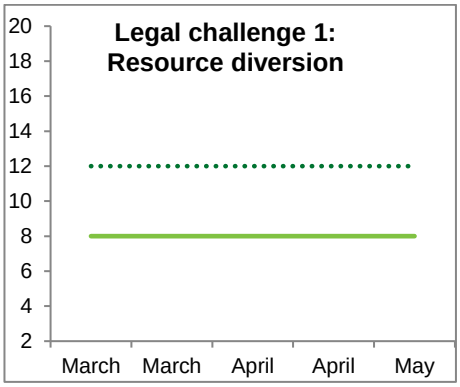


Lower and below tolerance risks









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
	Likelihood				

Risk Score = Impact x Likelihood

Risk appetite and tolerance

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

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

Assessing inherent risk

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

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

System-wide risk interdependencies

As of April 2017, we explicitly consider whether any HFEA strategic risks or controls have a potential impact for, or interdependency with, the Department or any other ALBs. A distinct section to record any such interdependencies beneath each risk has been added to the risk register, so as to be sure we identify and manage risk interdependencies in collaboration with relevant other bodies, and so that we can report easily and transparently on such interdependencies to DHSC or auditors as required.

Contingency actions

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

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

Audit and Governance Committee Forward Plan

Strategic delivery:	☐ Setting standards	☐ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	Audit & Governance Committee Forward Plan		
Agenda item	14		
Paper number	AGC (18/06/2016) 683 MA		
Meeting date	18 June 2019		
Author	Morounke Akingbola, Head of Finance		
Output:			
For information or decision?	Decision		
Recommendation	The Committee is asked to review and make any further suggestions and comments and agree the plan and to note the Cabinet Office: Counter Fraud one-of item has been removed. This item will be reported upon at each meeting in line with GovS 013		
Resource implications	None		
Implementation date	N/A		
Organisational risk	☒ Low	☐ Medium	☐ High
	Not to have a plan risks incomplete assurance, inadequate coverage or unavailability key officers or information		
Annexes	N/A		

Audit & Governance Committee Forward Plan

AGC Items Date:	5 Mar 2019	18 Jun 2019	8 Oct 2019	3 Dec 2019
Following Authority Date:	13 Mar 2019	3 July 2019	13 Nov 2019	Jan 2020
Meeting 'Theme/s'	Finance and Resources	Annual Reports, Information Governance, People	Strategy & Corporate Affairs, AGC review	Register and Compliance, Business Continuity
Reporting Officers	Director of Finance & Resources	Director of Finance & Resources	Director of Strategy & Corporate Affairs	Director of Compliance and Information
Strategic Risk Register	Yes	Yes	Yes	Yes
Digital Programme Update	Yes	Yes	Yes	Yes
Annual Report & Accounts (inc Annual Governance Statement)	Draft Annual Governance Statement	Yes – For approval		
External audit (NAO) strategy & work	Interim Feedback	Audit Completion Report	Audit Planning Report	Audit Planning Report
Information Assurance & Security		Yes		
Internal Audit Recommendations Follow-up	Yes	Yes	Yes	Yes
Internal Audit	Update	Results, annual opinion approve draft plan	Update	Update
Whistle Blowing, fraud (report of any incidents)	Update as necessary	Update as necessary	Update as necessary	Update as necessary
Contracts & Procurement including SLA management	Update as necessary	Update as necessary	Update as necessary	Update as necessary

AGC Items Date:	5 Mar 2019	18 Jun 2019	8 Oct 2019	3 Dec 2019
HR, People Planning & Processes		Yes Including bi-annual HR report		Bi-annual HR report
Strategy & Corporate Affairs management			Yes	
Regulatory & Register management	Yes			Yes
Cyber Security Training			Yes	
Resilience & Business Continuity Management	Yes	Yes	Yes	Yes
Finance and Resources management	Yes			
Reserves policy			Yes	
Anti-Fraud, Bribery and Corruption policy	*Reviewed and will be presented annually together with GovS 013 Counter Fraud*			
Public Interest Disclosure (Whistleblowing) policy	*Reviewed and will be presented annually*			
Estates	Yes	Yes	Yes	Yes
General Data Protection Act (GDPR)			Yes	Yes
Review of AGC activities & effectiveness, terms of reference				Yes
Legal Risks			Yes	
AGC Forward Plan	Yes	Yes	Yes	Yes
Session for Members and auditors	Yes	Yes	Yes	Yes

AGC Items Date:	5 Mar 2019	18 Jun 2019	8 Oct 2019	3 Dec 2019
~~Other one-off items~~	~~Cabinet Office Counter Fraud Standards~~ ~~Whistle Blowing Policy Review~~			

Government Functional Standards – Counter Fraud

Strategic delivery:	☐ Safe, ethical, effective treatment	☐ Consistent outcomes and support	☒ Improving standards through intelligence
Details:			
Meeting	AGC		
Agenda item	15		
Paper number	HFEA (12/06/2019) 684 MA		
Meeting date	18/06/2019		
Author	Morounke Akingbola, Head of Finance		
Output:			
For information or decision?	For information		
Recommendation	Note progress		
Resource implications			
Implementation date	02/09/2019		
Communication(s)			
Organisational risk	☐ Low	☒ Medium	☐ High
Annexes	Annex A: Assessment against Basic Standard Annex B: Government Functional Standards		

1. Background

1.1. In January 2019 the Cabinet Office launched a revised Functional Standards for Counter Fraud (GovS 013) and announced its extension to all ALBs. Assessment against these standards formed part of our recent Internal Audit review of the HFEA's counter fraud processes.

1.2. The purpose of the government functional standard is to set expectations for the management of fraud, bribery and corruption risk in government organisations. The standard represents the minimum that organisations should have in place and will evolve over time.

1.3. The Cabinet Office objectives include promoting a change in culture, improving capability, activity and resilience across Government and 100% of organisations to achieve basic level by the end of 2019.

1.4. The processes to achieve the above include assessments against the 'counter fraud elements' of Government Functional Standards (GovS 013) and from April 2020, the bribery and corruption elements. Departments and ALBs performance are to be published separately. A copy of the Standards are attached at Annex B

2. What this means for us

2.1. Compliance with these standards is a significant element of our response to the recent audit recommendations and will provide the organisation with a benchmark against which we can assess our counter fraud activities and approach. Our initial assessment is that the HFEA is currently operating at the **non-compliance** maturity level.

2.2. We are obliged to provide evidence to the Cabinet Office of our organisation's compliance with the standards by **2 September 2019.**

2.3. Cabinet Office will assess our evidence against these standards and will assign us a maturity level indicating how sophisticated we are in our approach. As a minimum they expect us to meet the 'basic' maturity level (i.e. we meet the standard). The results of their assessment will be published in their Fraud Landscape Review.

2.4. DHSC Anti-Fraud Unit have offered proportionate, risk-based support to help us meet Cabinet Office expectations. This builds on our previous engagement with the DHSC team.

2.5. The committee are invited to comment on our self-assessment against the standard at Annex A and plans to reach the required position by September 2019.

12 Standards Cabinet Office require ALBs to have in place by 2 September 2019

Standard	Criteria to meet the standard	DHSC's tips	Standard met?	HFEA response	Start date	End date
1. An **accountable individual** at board level who is responsible for counter fraud.	The organisation has an accountable individual in post at Director General level or equivalent to oversee the delivery of the organisation's counter fraud strategy	Equivalent DG	*No*	*We are yet to appoint an accountable individual. This will be put before the AGC /Authority?*	**18-06-2019 AGC meeting**	**18-06-2019**
2. The organisation has a **counter fraud strategy**	The organisation has a strategy in place that meets all aspects of GovS 013. The strategy has been approved by the board or executive risk committee	"Depending on how the organisation is structured and how it intends to meet the standard. Some smaller ALBs may have a single overarching approach which aligns with the core Department i.e. use DHSC's if you do not have your own	*No*	*No strategy in place. We would look to utilise DHSC's strategy and tailor to our needs.*	**June 2019**	**End July**
3. The organisation has an **annual action plan** that details the key actions to be taken to deliver the strategy or specific parts of it.	The organisation has an annual action plan that meets all aspects of GovS 013. The plan is tracked and monitored to ensure delivery.	Use template Not BAU Summarises key actions to improve capability, activity and resilience in that year Must include inter-dependencies with other ALBs.	*No*	*Dependent on when our strategy is written.*	**June 2019**	**End July**

Standard	Criteria to meet the standard	DHSC's tips	Standard met?	HFEA response	Start date	End date
4. The organisation has **outcome-based metrics** against the agreed actions for the financial year (including financial metrics where suitable).	The organisation has agreed targets/ outcomes and has metrics in place to monitor progress – these are regularly reviewed.	For organisations with 'significant investment' in counter fraud or 'significant estimated' fraud loss, these will include metrics with a financial impact – loss identified & prevented. If on-going fraud project forward a year or less if something else would have stopped it. For fraud headed off from the outset need a baseline – NHSCFA developing ideas on this Use for ARC reporting	*No*	*For discussion with AGC as this would be challenging to achieve.*		
5. The organisation has a **fraud risk assessment** (undertaken in accordance with the fraud risk assessment professional standard and guidance).	The organisation has undertaken a fraud risk assessment that meets all aspects of GovS 013. Fraud risks are clearly identified, carry an inherent risk rating, controls are described with narrative on how they mitigate the risk. Residual risk has been assessed and rated and there is a narrative on the risk that remains.	Use template Internal and external-facing risks (i.e. bank mandate)	*No*	*We have not undertaken a fraud risk assessment. We would look to conduct at high level initially in order to inform our return in line with Cabinet Office deadline*		

Standard	Criteria to meet the standard	DHSC's tips	Standard Met?	HFEA response	Start date	End date
6. The organisation has a **policy and response plan** for dealing with potential instances of fraud.	The organisation has a policy and response plan that fully covers the requirements of GovS 013.	Use GovS 013 roles and responsibilities for your policy, tweaking as appropriate.	*Partially*	*Counter Fraud and Anti-Theft policy with suggested response plan. There are some aspects of the Standard that need to be included.*	19 June	01 July
7. The organisation has well established and documented **reporting routes** for staff / contractors and members of the public to report fraud and **system(s) for recording referrals and allegations.**	The organisation has reporting routes and systems in place for recording instances of suspected fraud (referrals and allegations).	To record suspected fraud accredited investigators should use NHSCFA's case management system	Partially	Whistleblowing policy is in place; however, we may need to link this to our fraud policy		July
8. The organisation **reports quarterly** identified loss from fraud and error, alongside associated recoveries and prevented fraud to Cabinet Office inline with the agreed government definitions	The organisation reports losses to the Cabinet Office in line with the agreed government definitions using CDR	Use reports for ARC	*No*	Verbal updates are provided to AGC at meetings. We will formalise this process in order to comply. We are mandated to report to Cabinet Office by 2 September 2019.	June-19	Aug-19

Standard	Criteria to meet the standard	DHSC's tips	Standard Met?	HFEA response	Start date	End date
9. The organisation has access to **trained investigators** that meet the public sector skill standard (either directly or employees, has access to via another department	The organisation has access to trained investigators or employs investigators that meet the public sector skill standard.	DHSC AFU	*Yes*	We have access to DHSC AFU	N/a	N/a
10. The organisation undertakes activity to try and **detect fraud** in high risk areas where little is known of fraud levels. This can include loss measurement activity (FMA) or the use of data sharing analytics.	The organisation undertakes loss measurement activity through the FMA programme (or locally) and/or is proactive in using data and fraud data analytics to detect fraud.		*No*	No current access to data analytics. As with standard no.5.4 we would wish to discuss a proportionate response to this, given our size and available resources.		
11. Staff have access to and undertake **fraud awareness training** as appropriate to their role.	All staff have access to fraud awareness training and there is provision for role specific training where required.	We have materials which we will share. We will share contact details of ALBs, so you can share resources.	*No*	Fraud awareness training is available on Civil Service Learning (CSL) and will be shared with staff. Training to be mandatory and annually undertaken.	Jun-19	Aug-19
12. The organisation has policies and registers for **gifts and**	The organisation has registers and policies in place and staff disclose gifts, hospitality and	Please obtain assurances these are kept up to date, reviewed and action	*Yes*	Policy has been in place but not updated recently. A register is kept (in a book) and will be transferred to a spreadsheet.	Jun-19	Jun-19

hospitality and conflicts of interest.	conflicts of interest in line with the agreed policy.	taken if conflicts are identified.		Reminders will be sent to staff in line with annual reporting.		

NHS CFA – NHS Counter Fraud Authority
DHSC AFU – Department of Health and Social Care Anti-Fraud Unit
CDR – Consolidated Data Request
FMA – Fraud measurement and assurance

HM Government

Government Functional Standard

GovS 013: Counter fraud

Counter fraud, bribery and corruption

Version: 1.0
Status: Approved for internal government trial
Date issued: 11 Oct 2018

This standard is part of a suite of operational standards that sets expectations for management within government. Standards may include both mandatory and advisory elements. The following conventions are used to denote the intention:

Term	Intention
shall	denotes a requirement: a mandatory element
should	denotes a recommendation: an advisory element
may	denotes approval
might	denotes a possibility
can	denotes both capability and possibility
is/are	denotes a description

The meaning of words is as defined in the Shorter Oxford English Dictionary, except where defined in the Glossary in **Annex B**.

It is assumed that legal and regulatory requirements shall always be met.

© Crown copyright 2018

Produced by the Centre of Expertise for Counter Fraud, part of the Cabinet Office.

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence.
To view this licence, visit http://www.nationalarchives. gov.uk/doc/open-government-licence/ or email: psi@nationalarchives.gsi.gov.uk

Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned.

Alternative format versions of this report are available on request from the Centre of Expertise for Counter Fraud: fed@cabinetoffice.gov.uk

Contents

1. About this government functional standard

1.1. Purpose of this standard

The purpose of this government functional standard is to set the expectations for the management of fraud, bribery and corruption risk in government organisations.

This standard provides direction and guidance for:

- permanent secretaries, directors general, chief executive officers and chief financial officers of government departments and arms-length bodies
- counter fraud leads within organisations who manage fraud, bribery and corruption risk
- members of audit and risk committees
- audit and assurance bodies

Note: This standard builds upon the functional standards for counter fraud. The standard represents the minimum that organisations should have in place and will evolve over time.

Note: The functional standards for counter fraud were developed by a senior group of fraud experts in government. They were approved by the finance leaders group and were launched by the minister for the constitution in 2017.

1.2. Scope of this standard

This standard applies to all government departments and their arms-length bodies.

1.3. Government standards references

This standard should be used as a standalone government functional standard.

2. Principles

At all times, those responsible for counter fraud, bribery and corruption shall ensure:

1. accountabilities and responsibilities for managing fraud, bribery and corruption risk are defined across all levels of the organisation
2. staff have the skills, awareness and capability to protect the organisation against fraud, bribery and corruption
3. controls are in place to mitigate fraud, bribery and corruption risks and are regularly reviewed to meet evolving threats
4. fraud risk management practices, tools and methods continue to evolve in line with industry trends, threats and best practice
5. the standard is applied in accordance with the professional standards and guidance for counter fraud, bribery and corruption [1]
6. public service codes of conduct and ethics, and those of associated professions are upheld

3. Context

3.1. Introduction

Fraud is a significant risk to the UK public sector and has far-reaching financial and reputational consequences. The government estimates that fraud costs the public sector between £31bn and £49bn per year and much of this goes undetected.

The national audit office has challenged the government to do more because fraud is a hidden crime. In addition, serious and organised economic crime is a national security issue.

All government organisations should manage the risk of fraud, bribery and corruption in accordance with this standard.

4. Governance

4.1. Strategy

Organisations should have a counter fraud, bribery and corruption strategy.

The organisation's board or executive risk committee should approve the strategy.

Note: This may consist of a single overarching strategy or separate strategies (counter fraud as one, bribery and corruption as the other) depending on how the organisation is structured.

The strategy should describe how the organisation will develop its arrangements to counter fraud, bribery and corruption over 2 to 5 years, including:

- an assessment of the main risks and challenges facing the organisation
- an assessment of how the fraud landscape may change
- where the organisation wants to be in the next 2 to 5 years
- how it will actively counter fraud, bribery and corruption and develop its response
- objectives for the period of the strategy

The strategy should be informed by a fraud, bribery and corruption risk assessment and remain relevant to changes in the internal and external environment.

4.2. Annual action plan

Organisations should have an annual action plan that summarises key actions to improve capability, activity and resilience in that year.

The action plan should be linked to the strategy and detail the key actions to be taken to deliver the strategy or specific parts of it.

The annual action plan should target areas of improvement, as opposed to business as usual activity.

The annual action plan should:

- describe clearly the key activity that will be undertaken
- state what the timescales for delivery are
- state who the responsible owner(s) is/are
- state what the targeted outcome(s) will be
- be tracked and managed, so that progress against the plan can be monitored and reviewed

Organisations should submit their annual action plan to the centre of expertise for counter fraud prior to the start of the financial year and supply quarterly progress updates.

4.3. Outcome based metrics

Organisations should have outcome based metrics summarising what outcomes they are seeking to achieve that year. For organisations with 'significant investment' in counter fraud or 'significant estimated' fraud loss, these should include metrics with a financial impact.

Note: 'Significant investment' is defined as the level of expenditure allocated to counter fraud as a proportion of the gross expenditure limit or level of fraud loss incurred. Whether an organisation has a 'significant investment' in counter fraud is agreed between the organisation and the cabinet office centre of expertise for counter fraud.

Key activities planned should have defined outcomes and be measured using metrics that have quantifiable baselines or targets.

Organisations should have metrics for both business as usual and change activity as detailed in the annual action plan. Where there is a significant investment in counter fraud or a significant estimate of fraud loss, metrics should be financial, based on a targeted level of fraud prevented and/or detected in the financial year or a reduction in the estimated loss.

For organisations seeking to find more fraud, they should have metrics that target an increased level of referrals or value of fraud detected and/or prevented.

4.4. Roles and responsibilities

Responsibilities for key tasks with regard to counter fraud, bribery and corruption should be defined and have identifiable and appropriate people assigned to them, including someone to whom each person is responsible. Each role should have a clear path to accountability and the reporting lines should be documented.

4.4.1. The centre of expertise for counter fraud

The centre of expertise for counter fraud provides leadership and guidance on what government organisations should do to counter fraud, bribery and corruption. It is responsible for understanding the pan-government landscape on fraud, economic crime, error loss and capability, and works across government to deal with the challenges in this area.

The centre supports the development of counter fraud capability in government through the government counter fraud profession.

The centre also:

- develops, maintains and provides assurance over this functional standard
- provides expert advice and support to government organisations
- delivers services which the public sector can use
- maintains the evidence base and publishes data on the levels of fraud in government, and compliance with this standard
- engages with government organisations to share best practice at home and abroad
- monitors and agrees targets to reduce loss in areas of significant loss

4.4.2. Accountable individual in government organisations

Organisations shall have an accountable individual at board level who is responsible for counter fraud, bribery and corruption.

The accountable board member should provide effective leadership to ensure the organisation is managing the risk of fraud, bribery and corruption. In discharging that responsibility they should:

- work with the organisation to meet this functional standard, and make the board aware of where there are gaps
- be accountable to the board for the organisation's performance in countering fraud, bribery and corruption
- ensure the board has discussions on the nature of fraud risk in the organisation, and how it is being dealt with
- ensure accountability for fraud risk and loss in areas of the organisation and services are clearly understood across the organisation
- ensure the organisation has the resources, skills and capability to deliver to the counter fraud, bribery and corruption strategy

It is possible for this accountability to be split between different board members. However, where this is the case, those with accountability should be accountable for specific areas of the business (rather than have joint accountability), and this accountability should be recorded and recognised by the board.

Note: Board level accountability will vary between organisations and may include permanent secretaries.

4.4.3. Senior lead for counter fraud in government organisations

The board member should ensure the organisation has a lead with day-to-day responsibility for counter fraud, bribery and corruption. In discharging that responsibility they should:

- work with the organisation to meet this functional standard
- have a detailed understanding of the fraud, bribery and corruption risks that the organisation faces and an effective method for communicating these
- have a good understanding of the organisation, and the context within which it operates, alongside the limitations it may have in dealing with fraud, bribery and corruption
- have an understanding of the organisation's fraud controls, their effectiveness and limitations
- devise, manage and implement the organisation's counter fraud, bribery and corruption strategy
- be responsible for developing capability within the organisation, ensuring staff have the skills and capability necessary to deliver the counter fraud, bribery and corruption strategy, policy and response plan
- actively seek out best practice on counter fraud, bribery and corruption and integrate it into the practices of the organisation and their delivery partners

Note: Different organisations have different arrangements in place for this role. Some have full-time leads with experience in working in counter fraud. These individuals can be responsible for the organisation's counter fraud unit, function or activity. However, this is not always the case. In other organisations an individual takes on this role as part of their wider responsibilities.

Some, larger organisations may have several senior leads covering different areas. In these cases, each lead should have clear areas of responsibility agreed with the accountable individual.

In line with the UK's anti-corruption strategy [6] all government departments shall have a senior counter fraud lead who is a member of government counter fraud profession by 2022 [4].

4.4.4. Counter fraud champions in government organisations

All organisations should nominate an individual to be their counter fraud champion. The individual should be of sufficient seniority to be able to communicate and have access to the whole organisation. The champion and the organisational senior lead for counter fraud can be the same person, although they do not need to be. In discharging that responsibility they should:

- promote awareness of fraud, bribery and corruption within their organisation
- understand the threat posed from fraud, bribery and corruption
- understand best practice on counter fraud
- understand cross government fraud initiatives and engage their organisation, and any associated organisations, in those initiatives

4.4.5. Individual staff members in government organisations

Individual staff members have a responsibility to perform their roles in accordance with the civil service code [7]. The code expects civil servants to operate with integrity and to comply with all laws (including the Fraud Act, Bribery Act and any subsequent legislation).

In performing their role, and in meeting this standard, they should:

- undertake fraud, bribery and corruption training as defined by their organisation
- report any reasonable suspicion of fraud, bribery and corruption using the reporting routes as defined by their organisation
- adhere to the fraud and corruption policy and response plan as defined by their organisation
- adhere to the gifts and hospitality and conflicts of interests policy as defined by their organisation.

4.5. Annual assurance

Organisations should evidence against this standard to the centre of expertise for counter fraud annually.

The centre of expertise for counter fraud carries out an annual assurance check to determine the compliance level in government. The results of which are published and are used to improve performance.

5. Counter fraud, bribery and corruption practices

5.1. Fraud risk assessments

Organisations should have a fraud, bribery and corruption risk assessment.

This should be undertaken in line with the practice detailed in the fraud risk assessment professional standards and guidance [2].

The organisation should undertake varying levels of risk assessments including:

- a high-level fraud, bribery and corruption risk assessment that gives an overview of the main risks and challenges facing the organisation to the board
- an intermediate fraud, bribery and corruption risk assessment that extends to departmental functions, programmes or major areas of spend
- a detailed fraud, bribery and corruption risk assessment that covers individual business units, projects or programmes

Organisations should have a high-level risk assessment and some detailed risk assessments in the highest risk areas. Intermediate assessments are advisable in larger organisations with a wide range of payment or service streams.

Organisations should undertake fraud, bribery and corruption risk assessments on a regular basis. They should be seen as an on-going process, rather than a standalone exercise.

5.2. Policy and response plans

Organisations should have:

- a fraud, bribery and corruption policy, and
- a response plan for dealing with potential instances of fraud, bribery and corruption

The policy should set out:

- what the standards of expected behaviour are, including how they align to the civil service code [see principle 6]
- how fraud and corruption is defined in the organisation with reference to current legislation and government definitions
- a clear statement of how the organisation deals with fraud, bribery and corruption, including activity they undertake to find fraud
- a statement on the organisations approach to fraud risk assessment
- what staff and management responsibilities are for fraud, bribery and corruption, including who is responsible for what areas of the organisation
- how the organisation will continue to improve based upon lessons learnt

The policy should be a restricted document, as it will contain sensitive information that may increase the risk of fraud and economic crime to the organisation if it is made public.

The response plan should set out:

- where individuals can report potential instances of fraud and corruption
- how the organisation deals with individual items of intelligence from these, and other, referrals

- how the organisation responds to instances of fraud, bribery and corruption
- how the organisation monitors the progress of any investigations, and takes decisions on them
- the roles and responsibilities staff, teams and individual functions in responding to an instance of fraud, bribery and corruption
- how this information will be reported, both within the organisation, and to other relevant organisations

5.3. Reporting routes

Organisations should have well established and documented reporting routes for staff, contractors and members of the public to report suspicions of fraud, bribery and corruption and a mechanism for recording these referrals and allegations.

Reporting routes should be published and promoted. Organisations should monitor the usage of these reporting routes, and consider whether they are effective.

Organisations should have a mechanism or system for recording all reported potential instances of fraud, bribery and corruption. Instances should be recorded so the specifics of the allegations are clearly identified, including any individuals and/or organisations involved and the act(s) they are alleged to have undertaken.

5.4. Loss reporting

Organisations should report identified loss from fraud, bribery, corruption and error, alongside associated recoveries and prevented losses, to the centre of expertise for counter fraud, in line with the agreed government definitions [5].

Losses and recoveries should be reported using a consolidated data request (CDR) in accordance with the timescales set by cabinet office.

Loss reporting frequency may change depending on the need to conduct detailed fraud loss and error reviews. Any changes on frequency will be consulted with organisations.

Organisations should store their data on fraud, bribery and corruption loss in a manner that is conducive to quick reporting and analysis.

Note: The government's standard definitions for fraud loss and error reporting have been agreed across government and are available from the centre of expertise for counter fraud.

5.5. Access to trained investigators

Organisations should have access to trained investigators that meet the public sector skill standard. See investigation core discipline standard [3].

The investigation core discipline standard details the skills, knowledge and experience that those who investigate fraud and economic crime should have. Organisations should take steps to ensure they have access to investigators who meet these standards.

Note: The government counter fraud profession, based on the investigation standards (and other standards) will be introduced in 2018. Over time, organisations will be able to formally assess their investigative resources against these standards.

5.6. Proactive detection activity

Organisations should undertake activity to try and detect fraud in high-risk areas where little or nothing is known of fraud, bribery and corruption levels. This activity should include using loss measurement activity (fraud measurement and assurance) where suitable.

Proactive detection activity can include using fraud measurement and assurance activity, or the use of new data sharing and analytics to attempt to find fraud in a specific area, based on a good understanding of the risks in that area.

5.7. Fraud, bribery and corruption awareness training

Organisations should ensure staff have access to, and undertake, fraud awareness, bribery and corruption training as appropriate to their role.

Individual staff members should ensure completion of counter fraud, bribery and corruption training as set by the organisation.

The senior lead for counter fraud within the organisation is responsible for the provision of fraud, bribery and corruption training. The accountable individual is responsible for the decision on what training is appropriate.

5.8. Policies and registers for gifts and hospitality and conflicts of interest

Organisations should have policies and registers for gifts and hospitality and conflicts of interest.

Staff should declare offers of gifts and hospitality (whether accepted or declined) in accordance with the gift and hospitality policy that is set down by the organisation.

Offers of gifts and hospitality (whether accepted or declined) should be recorded within the gifts and hospitality register.

Staff should declare any conflicts of interests in accordance with the conflicts of interest policy that is set down by the organisation.

Conflicts of interest should be recorded within the conflict of interest register.

A. References

ID	Description
1	Cabinet Office (2018) Government Counter Fraud Profession **https://civilservicelearning.civilservice.gov.uk/professions/counter-fraud-profession**
2	Cabinet Office (2018) Fraud Risk Assessment Core Discipline Standard **https://civilservicelearning.civilservice.gov.uk/professions/professions/counter-fraud-profession/professional-standards-guidance**
3	Cabinet Office (2018) Fraud Investigation Core Discipline Standard **https://civilservicelearning.civilservice.gov.uk/professions/professions/counter-fraud-profession/professional-standards-guidance**
4	Cabinet Office (2018) Fraud Leadership, Management and Strategy Core Discipline Standard **https://civilservicelearning.civilservice.gov.uk/professions/professions/counter-fraud-profession/professional-standards-guidance**
5	Cabinet Office (2018) Fraud Loss and Error Reporting Policy Policy and guidance is available from the Centre of Expertise for Counter Fraud
6	UK Anti-Corruption Strategy 2017 to 2022 **https://www.gov.uk/government/publications/uk-anti-corruption-strategy-2017-to-2022**
7	Civil Service (2015) The Civil Service Code **https://www.gov.uk/government/publications/civil-service-code/the-civil-service-code**

B. Glossary

Term	Definition
Fraud	Wrongful or criminal deception intended to result in financial or personal gain (as set out in the Fraud Act 2006 and any subsequent legislation).
Bribery	Dishonestly persuading someone to act in one's favour by a gift of money or other inducement (as set out in the Bribery Act 2010).
Corruption	The abuse of entrusted power, dishonest or fraudulent conduct for personal or political gain.
Lessons learnt	The practice of continuous improvement based upon organisational learning in a risk management context.
Organisation	In the context of government functional standards, 'organisation' is the generic term used to describe a government department, arm's length body, or any other entity, which is identified as being in scope of the functional standard.
Counter fraud strategy	A defined approach for how the organisation will counter fraud, bribery and corruption over a 2 to 5 year period.
Fraud annual action plan	A plan detailing the specific actions that an organisation will undertake to deliver the counter fraud strategy or specific parts of it within the financial year.
Fraud outcome based metrics	A method of measuring a particular task, activity or process using quantifiable measures based upon the outcome (i.e. financial savings, fraud rate, volume/value of fraud detected/prevented, false positive rate or percentage of staff trained)
Fraud reporting route	A communication channel or reporting medium for staff, contractors or members of the public to report fraud, bribery and corruption to the organisation (i.e. a whistleblowing line, fraud reporting hotline or online reporting service/tool).
Fraud and error loss reporting	The method of reporting loss data relating to fraud and error to the cabinet office using the consolidated data request process.
Fraud loss measurement	The method of selecting a sample to estimate the total cost of fraud or error.
Fraud assurance	The method of validating the level of fraud or error loss found.

C. Counter fraud organisational basics checklist

1. Have an **accountable individual** at board level who is responsible for counter fraud, bribery and corruption;
2. Have a **counter fraud, bribery and corruption strategy** that is submitted to the centre;
3. Have a **fraud, bribery and corruption risk assessment** that is submitted to the centre;
4. Have a **policy** and **response plan** for dealing with potential instances of fraud, bribery and corruption;
5. Have an **annual action plan** that summarises key actions to improve capability, activity and resilience in that year;
6. Have **outcome based metrics** summarising what outcomes they are seeking to achieve that year. For organisations with 'significant investment' in counter fraud or 'significant estimated' fraud loss, these will include metrics with a financial impact;
7. Have well established and documented **reporting routes for staff, contractors and members of the public** to report suspicions of fraud, bribery and corruption and a mechanism for recording these referrals and allegations;
8. Will **report identified loss** from fraud, bribery, corruption and error, and associated recoveries, to the centre in line with the agreed government definitions;
9. Have agreed **access to trained investigators** that meet the agreed public sector skill standard;
10. Undertake **activity to try and detect fraud** in high-risk areas where little or nothing is known of fraud, bribery and corruption levels, including loss measurement activity where suitable;
11. Ensure all staff have **access to and undertake fraud awareness, bribery and corruption training as appropriate to their role;**
12. Have **policies and registers for gifts and hospitality and conflicts of interest.**

design102 Find out more at design102.co.uk
Design that makes a difference