# Audit and Governance Committee meeting - agenda

## 12 June 2018

## Abbey Room

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

| | Agenda item | | Time |
|---|---|---|---|
| 1. | Welcome, apologies and declaration of interests | | 10:00am |
| 2. | Minutes of 5 March 2018<br>**[AGC (12/06/2018) 600]** | For Decision | 10.05am |
| 3. | Matters Arising<br>**[AGC (12/06/2018) 601 MA]** | For Information | 10.10am |
| 4. | Internal Audit | | 10.15am |
| | a) Annual Assurance Statement 2017-18<br>**[AGC (12/06/2018) 602 DH]** | For Information | |
| | b) 2018/19 Plan<br>**[AGC (12/06/2018) 603 DH]** | For Information | |
| 5. | Implementation of Recommendations<br>**[AGC (12/06/2018) 604 MA]** | For information | 10.25am |
| 6. | Annual Report and Accounts<br>**[AGC (12/06/2018) 605 RS]** | For Approval | 10.35am |
| 7. | External Audit – Audit Completion Report<br>**[AGC (12/06/2018) 606 NAO]** | To Follow | 11.00am |
| 8. | HR, People, Planning and Processes | | 11.10am |
| | a) HR Strategy<br>**[AGC (12/06/2018) 607 PT]** | Presentation | |
| | b) Review of the Organisational Change Implementation<br>**[AGC (12/06/2018) 608 PT]** | Presentation | |
| | c) Estates Update<br>**[AGC (12/06/2018) 609 RS]** | Verbal Update | |

| | | | |
|---|---|---|---|
| 9. | Digital Programme Update<br>**[AGC (12/06/2018) 610 DH]** | For Information | 11.40am |
| 10. | Resilience, Business Continuity Management Cyber Security<br>**[AGC (12/06/2018) 611 DH]** | For Information | 12.05pm |
| 11. | Strategic Risk Register<br>**[AGC (12/06/2018) 612 HC]** | For Information/Comment | 12:30pm |
| 12. | AGC Forward Plan<br>**[AGC (12/06/2018) 613 MA]** | For Decision | 12.40pm |
| 13. | Whistle Blowing and Fraud<br>**[AGC (12/06/2018) 614 RS]** | Verbal update | 12.45pm |
| 14. | Contracts and Procurement<br>**[AGC (12/06/2018) 615 MA]** | Verbal update | 12.50pm |
| 15. | Any other business | | 12.55pm |
| 16. | Close (Refreshments & Lunch provided) | | 1.00pm |
| 17. | Session for members and auditors only | | 1.00pm |
| 18. | Next Meeting 10am Tuesday, 9 October 2018, HFEA Offices, London | | |

# Audit and Governance Committee meeting minutes

| | | | |
|---|---|---|---|
| **Strategic delivery:** | ☐ Setting standards | ☐ Increasing and informing choice | ☐ Demonstrating efficiency economy and value |

| **Details:** | |
|---|---|
| Meeting | Audit and Governance Committee |
| Agenda item | 2 |
| Paper number | AGC (12/06/2018) 600 |
| Meeting date | 12 June 2018 |
| Author | Bernice Ash, Committee Secretary |
| **Output:** | |
| For information or decision? | For decision |
| Recommendation | Members are asked to confirm the minutes as a true and accurate record of the meeting |
| Resource implications | |
| Implementation date | |
| Communication(s) | |
| Organisational risk | ☐ Low ☐ Medium ☐ High |
| Annexes | |

## Minutes of Audit and Governance Committee meeting held on 6 March 2018

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

| | |
|---|---|
| Members present | Margaret Gilmore (Chair)<br>Anita Bharucha (by teleconference)<br>Mark McLaughlin<br>Geoffrey Podger |
| Apologies | Helena Long – National Audit Office (NAO) |
| External advisers | Jeremy Nolan – Head of Internal Audit<br><br>External Audit - National Audit Office (NAO):<br>George Smiles |
| Observers | Kim Hayes, Department of Health |
| Staff in attendance | Peter Thompson, Chief Executive<br>Morounke Akingbola, Head of Finance<br>Richard Sydee, Director of Finance and Resources<br>Nick Jones, Director of Compliance and Information<br>Paula Robinson, Head of Planning and Governance<br>Helen Crutcher, Risk and Business Planning Manager<br>Dan Howard, Chief Information Officer<br>Nana Gyamfi, Licensing Information Officer<br>Aleksandra Deja, Information Governance Project Manager<br>Bernice Ash, Committee Secretary |

## 1. Welcome, apologies and declarations of interests

**1.1** The Chair welcomed attendees to the meeting.

**1.2** Apologies were received from Helena Long, National Audit Office.

**1.3** There were no declarations of interest.

## 2. Minutes of the meeting held on 5 December 2017

**2.1** The minutes of the meeting held on 5 December 2017 were agreed as a true record and approved for signature by the Chair.

## 3. Matters arising

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

**3.2** Items 11.6, 8.5 and 9.11 relating to updates on cyber security, access to Office 365 and reporting of cyber security issues to the relevant Authority member are ongoing; it was agreed these could be removed from the matters arising log.

**3.3** 9.12) The Head of Finance confirmed that 98% of staff had now completed the cyber security training. The remaining 2% was accounted for by means of four staff on maternity leave and one individual currently encountering technical issues accessing the training. It was agreed this item could be removed from the matters arising log. The Committee agreed it would be useful to receive periodic reviews on this issue, particularly at times of high staff turnover. The Head of Planning and Governance would also reissue the link for this training to Authority Members.

**3.4** 12.7) The NAO reported on training undertaken for a similar committee at the Human Tissue Authority, providing an overview of the NAO work programme and their perspective on the challenges facing the NHS. The Committee agreed it would be useful for them to receive the same training.

**3.5** 12.8) Training for members had been deferred and the Director of Finance and Resources will seek to schedule this to occur during the members private session, after the autumn meeting.

**3.6** Items 15.2, 6.6, 4.18, 8.8, 9.9, and 9.10 relating to the fraud investigation, training plan for the Committee, updates on regulatory and Register management, Brexit, alongside assurance points and progress updates relating to the Digital Programme, have been addressed in the items on the agenda below.

## Actions

**3.7** The Chief Information Officer to ensure the Committee receive periodic reviews on the position, regarding staff completion of cyber security training, particularly at times of high staff turnover.

**3.8** The Head of Planning and Governance to reissue the cyber security training link to Authority members.

**3.9** The Director of Finance and Resources to liaise with the NAO regarding training to Committee members, providing an overview of the NAO work programme and their perspective on the challenges facing the NHS.

# 4. Finance and Resources Update

**4.1** The Director of Finance and Resources provided the Committee with a presentation covering income, expenditure, the joint resources directorate review and finance and estates risks.

**4.2** The Committee noted that income for the Authority, in 2017/18 was c£6.3m, with c£5.3m of this generated from licence fees and £0.09m GIA from the Department of Health and Social Care (DHSC). It was identified that the sum received from the DHSC had reduced considerably over last few years.

**4.3** The Director of Finance and Resources referred to historic treatment trends, observing that the number of treatment cycles have been steadily rising since the creation of the Authority in 1991. In the last ten years, there has been an increase in treatments of around 2% per annum; this represents a significant growth in general demand. The Committee noted that demographic data confirms that an increasing number of people now have their first child in their 30s or 40s.

**4.4** The Committee noted that the Authority's current fees for centres stand at £80 for each cycle of IVF and £37.50 for each cycle of donor insemination. The cost of IVF treatment is very expensive, within a competitive market. A price drop for IVF treatment could result in further people accessing this service.

**4.5** The budget for the Authority in 2017/18 is c£6m, with almost two thirds of spend on salary costs. Legal and facilities costs represent a further 20% of the total spend. 15% of the total spend is non-discretionary, covering Authority and Committee meetings, inspections, and IT licences and consumables. It was noted that at start of each financial year, only 5% of the spend (c£300k) is truly discretionary, in that there is not a contractual or legal obligation for the Authority to undertake the expenditure. This remaining sum is primarily used for staff training, external communications and publications. It was suggested that any emerging surplus could be used in a value-added way within the sector.

**4.6** The Committee noted there had been a joint finance and resources post, for the Authority and the Human Tissue Authority (HTA) since 2014, following the McCracken review. The Director of Finance and Resources stated that overall, this approach works well and financial reporting is robust. However, it does pose some concern as it gives rise to a single point of failure and a heavy workload on specific roles. It was identified that perhaps more resource is needed at Executive level for ad hoc projects and oversight.

**4.7** The Committee noted the ten recommendations resulting from the joint resources directorate review, six of which focus internally on roles and responsibilities, better communication and more clarity on the scope of the Director role at both organisations. The remaining four recommendations relate to closer working in other corporate services such as HR, and the desire to explore a more strategic approach in terms of estates and other support areas across the Authority and the HTA, alongside other similar sized DHSC Arm's Length Bodies (ALBs).

**4.8** Regarding finance risks, there is limited concern over future income projections and expenditure plans in the short term. Medium term income will continue to be uncertain, but modelling will enable the Authority to better respond to emerging trends.

**4.9** In respect of estates risks, the Director of Finance and Resources highlighted the lease at Spring Gardens, ending in November 2020. The British Council, the main tenant in the building, will be relocating to Stratford ahead of this date and it is known that the government is seeking to relocate ALBs outside Zone 1. The Committee was informed that this is a significant risk for the Authority and a strategy to deal with this future relocation would be drawn up by the end of 2018. A further announcement from government, on the future approach to ALB locations, is expected in March 2018.

**4.10** The General Data Protection Regulation (GDPR), due to launch on 25 May 2018 was identified as another risk for the Authority.

**4.11** The Chair thanked the Director and the Head of Finance for their continued support, working within this joint resource directorate structure. The Chair questioned whether this joint resource approach provided more benefits than risk. The Chief Executive referenced the loss of a senior band post, but stated this has not created a huge problem. The current structure is workable and not an issue to be escalated to the DHSC Nevertheless, it does place a pressure on the individuals involved, particularly at specific times such as the end of the business year. The structure does increase the level of risk borne by the organisation.

**4.12** The Committee discussed the future relocation of the Authority, stating the importance of making the right move and retaining staff. The need to work in tandem with other ALBs was stated. It was identified that the creation of large hubs can result in higher rents. Being based in a location, with other ALBs in the DHSC community, can also result in both loss and gain of staff. The Committee agreed that it was important to know where current staff reside when considering the relocation.

**4.13** The Director of Finance and Resources stated that an item on estates would be a regular agenda item for future Committee meetings, and placed on the Forward Plan, from the end of 2018.

**4.14** The Committee acknowledged there had been no significant increase to staff salaries, in line with government pay restrictions, for several years, posing another risk to the Authority. The committee asked whether higher salaries could be funded from the organisation's own resources. The Director of Finance and Resources stated that some forecasting had been conducted, in respect of accommodation and staff salary costs, the costs would be affordable in the medium term but in the longer term wage inflation would outstrip forecast activity growth.

**4.15** The Chair stated that costs associated with legal risks cannot be underestimated and there is a real potential for more legal cases, particularly with the increasing range of treatments becoming available. Spending on inspections is also considerable.

**4.16** The Chief Executive spoke of the constraints placed on the Authority, being a government ALB, restricting the ability to pay staff more or to give further benefits to patients by using a surplus in the way suggested.

**4.17** The Director of Compliance and Information stated that, over the last two years, an intelligence led approach has been taken for inspections. Relatively, spending costs on inspections is quite small.

### Action

**4.18** The Director of Finance and Resources to add an item on estates to the Forward Plan, for regular discussion at Committee meetings, from the end of 2018.

## 5. Internal Audit

### a) Internal Audit Progress Report

**5.1** The Head of Internal Audit confirmed that the audit plan for 2017/2018 had been completed, with some follow-up work outstanding.

**5.2** The Head of Internal Audit summarised the findings from the review of Financial Controls and that the level of assurance had been assessed as substantive. The Chair of the committee welcomed the findings and congratulated the Resources Directorate on the report

**5.3** The Head of Internal Audit informed the Committee that the final report for the General Data Protection Regulation (GDPR) (an advisory review) had been issued on 27 February 2018 and work on the recommendations follow-up had commenced, with completion expected in mid-March 2018.

**5.4** The Director of Finance and Resources gave a presentation on the GDPR project, providing an overview, information about the project group and progress to date.

**5.5** The GDPR will come into force on 25 May 2018, presenting a significant challenge in terms of the handling of the data the Authority holds and the process of ensuring the right information, policies and procedures are in place to respect privacy in response to requests, alongside the internal roles required to oversee and manage the new approach to personal data. It was noted that GDPR does not supersede the responsibilities the organisation has under the HFE Act and other legislation to hold and process personal data held on the Register.

**5.6** A joint HTA/HFEA GDPR project group was instigated in November 2017 and had met on four occasions. The project group reports into Corporate Management Group meetings each month, alongside providing updates to the Senior Management Team.

**5.7** The Director of Finance and Resources reported the project group had agreed and adopted a single model as a road map for GDPR compliance, this being the Nymity Privacy Management Accountability Framework. This framework provides 72 questions, under 12 headings, that, if answered positively and supported by documentary evidence, should ensure that GDPR compliance is achieved. The 72 questions have been initially assessed and scored; 20 have been categorised at high risk, 33 as medium risk and 19 as low risk. Those marked as high risk must be complete by 25 May 2018. There needs to be a clear rationale, and therefore a defensible position, for those categorised as medium risk, if they are not completed by 25 May 2018. The remaining questions, assessed as low risk, are not directly relevant to the Authority or can be implemented after the GDPR launch data with little impact on the organisation's compliance position.

**5.8** The Committee noted that after an assessment of current progress, the Authority would not be fully compliant by the 25 May 2018 GDPR implementation date, and the organisation will need to prove it has a defensible position for this. It was noted that this will be a common scenario for many organisations across the public sector.

**5.9** The Director of Finance and Resources noted that the Committee are not scheduled to meet again until after the implementation date for GDPR, suggesting ways to provide sufficient assurance on progress against the plan towards compliance. This might include attendance/dial in to project meetings, specific teleconferences and document circulation.

**5.10** The Committee considered GDPR to be a significant business and reputational risk. The Committee requested to be made aware of any risks that might materialise, partaking in regular teleconferences as necessary. Assurance would also be required, in November 2018, that all the necessary compliances had been met.

**5.11** The Committee particularly referenced the recommendations made in the Internal Audit GDPR report, noting these to be a list of questions, asking if there are any other gaps.

**5.12** The Director of Finance and Resources would provide the Committee with an update report in mid-April 2018 and arrange a teleconference, if required, a week prior to the GDPR go live date.

**5.13** The Head of Internal Audit provided a summary of the audit topics for 2018/19. The topics chosen were business continuity, cyber security, the GDPR, risk management and governance and payroll and expenses. These were generally felt to be relevant and added value, although there was some discussion as to whether the risk management audit was the best use of resources.

**5.14** The Committee discussed whether fraud should be included as an audit topic for 2018/2019. The Head of Internal Audit agreed that an anti-fraud audit should be included instead of the risk management audit.

## Actions

**5.15** The Director of Finance and Resources to inform the Committee should any risks related to GDPR compliance materialise.

**5.16** The Director of Finance and Resources would provide the Committee with an update report in mid-April 2018 and arrange a teleconference, if required, a week prior to the GDPR go live date.

**5.17** The Head of Internal Audit to ensure that contractual risk is a focus point for the 2018/2019 audit programme.

### b) Progress with Audit Recommendations

**5.18** The Head of Finance reported on progress with audit recommendations, particularly noting, with regards to staffing/capability, the completion of the staff survey and the plans to provide quarterly or bi-annual reports to the Senior Management Team on general themes emerging from exit interviews. This audit recommendation should be completed by the end of the financial year, then removed from the schedule. The Head of Internal Audit would conduct a review of the evidence submitted, on the staffing/capability audit, and provide confirmation, by email to the Committee, if satisfied this can be removed from the schedule.

### Action

**5.19** The Head of Internal Audit to conduct a review of the evidence submitted on closed recommendations, and provide confirmation to the Committee by email, if satisfied.

## 6. External Audit – Audit Planning Report

**6.1** The NAO notified the Committee that the second internal audit was currently in progress and all work was being conducted to the planned timeframe.

## 7. Impact of Brexit

**7.1** The Chief Executive spoke to the paper regarding the potential impact of Brexit on the Authority, stating that the previously outstanding legislation, the Coding Directive (EC/2015/565) and the Import Directive (EC/2015/566), had now been approved by Parliament and will come into force on 1 April 2018, being fully incorporated into the HFE Act.

**7.2** The need to articulate what the Authority seeks to achieve and its impact on research, in the light of Brexit, has been identified. The Chief Executive, the Director of Compliance and Information and the Chair of the Authority had met with the European Society of Human Reproduction and Embryology to discuss issues associated with Brexit.

**7.3** The Committee raised some questions as to what might happen if Brexit does not progress as anticipated and the possibility of the Commission withdrawing support. The Chief Executive reported that the Commission had already distributed letters in respect of the issues raised by Brexit and the impact on imports and exports of gametes and embryos, noting that on exit from the EU, the United Kingdom would be treated as a 'third country'. After exit from the EU, some clinics would encounter difficulties in accessing gametes, resulting in longer waiting times and the need to approach sources in the USA. For contingency, there may be the need to look at different mechanisms for imports.

**7.4** The DHSC confirmed instructions were currently being drawn up for both Brexit and no Brexit scenarios and these will be shared with the Authority in the next few weeks, for input. However, it was noted that the issue of Brexit would have a larger impact on the HTA.

## 8. Digital Programme Update: Including Data Submission

**8.1** The Chief Information Officer spoke to the paper and presentation, providing a digital programme update regarding the system and the new register launch, programme milestones, data migration and cleansing, a risk review and finance and budget.

**8.2** The Committee particularly noted the review of the initial approach to the launch and the revised plan. A single implementation would now occur in September/October 2018. Communication and engagement will all parties was continuing and the new data submission system has been branded as PRISM.

**8.3** The Chief Information Officer stated that a firm, but fair approach, has been taken with third party system providers. Regarding the Azure environment, work had started to include areas such as auditing and network design. Penetration testing is scheduled for early April 2018. The Committee was informed of the programme milestones, noting the final data migration is scheduled for September 2018.

**8.4** The risk review was noted, with items relating to the complexity of data migration, the loss of key staff and pace of the project alongside the potential delay of rollout to the Electronic Patient Record System (EPRS) API.

**8.5** The Committee was informed that the project is delivering on target and within the agreed capital allocation. The financial outturn for 2017/2018 is forecast to be £324k, against the agreed capital budget of £350k.

*The Chair asked the observer attending from the Department of Health and Social Care to withdraw for the following discussion.*

**8.6** The Director of Compliance and Information stated that the data submission system is nearing completion and the organisation is now looking at its digital ambition with regard to the website and other internal systems. This work would continue into the next financial year, creating an additional cost.

**8.7** The final migration and launch of the new system is a huge technical exercise, requiring external support. The need to ensure that all necessary systems are correctly aligned was stated. Some of this work related to the overall reporting requirements for the Authority.

**8.8** The Director of Compliance and Information stated that the complete scope and cost of the digital programme work (formerly IfQ) had been underestimated. Original advice about this work led the Authority to believe this would be a comparatively small project, but it had realistically resulted in an additional £170k cost. The work had all been conducted securely but now other IT systems need updating.

**8.9** The Committee noted that the Authority usually receives £100k in capital cover from the DHSC per annum, but received an additional £350k last year. The Director of Finance and Resources and Head of Finance would be looking at the capital required from the DHSC, for 2018/19, over the next few weeks, but it was thought be in the region of £400k-£500k.

**8.10** The reputation and business risk associated with underinvesting in IT capital and assets was noted. It was crucial for the Authority to be certain of the figure required from the DHSC before approaching them. Comprehensive clarity on the amount required for IfQ completion work, and

that for systems investment, must be established. The need to be open and transparent was stated.

**8.11** The Committee asked the Executive to provide a detailed business case explaining the need to ask for further funding. The Committee supported the Executive's view that completing this work effectively is essential and that therefore approaching DHSC for extra funds was unavoidable – subject to a detailed explanation and specific figures being produced. It noted that the cost would be in the region of £500k. The Committee received assurances from the Executive that it would be kept informed of developments. The Committee thanked the Executive for the fast and transparent action it had taken in bringing this issue to the AGC.

*The observer from the DHSC re-joined the meeting.*

**8.12** The Chair summarised that the cost of the new systems and updating of old systems had been underestimated. Original advice received on the cost of the IT project had been incorrect as work had proved to be more complicated than anticipated. The Authority would be in a position to approach the DHSC with a new figure, including the estimated shortfall, in the next few weeks, but it was thought to be in the region of £500k.

**8.13** The Committee stated it had discussed the issues and challenged the Executive on the reasons associated with the emerging need for further funds, and had received satisfactory assurances. The Committee supported the Executive in its plan to request additional funding and urged the Executive to produce the detailed case and sums as soon as possible.

**8.14** The Authority will write formally to the DHSC regarding this matter. The issue would be presented at the forthcoming Authority meeting on 14 March 2018.

## Action

**8.15** The Committee to be kept informed of developments regarding capital requested from the DHSC and the response obtained.

## 9. Resilience, Business Continuity Management and Cyber Security

**9.1** The Chief Information Officer provided the Committee with a progress update regarding resilience, business continuity and cyber security.

**9.2** The Committee was notified that the Information Risk Training has been completed. Work is continuing in relation to the Microsoft Azure (cloud) server environment for the new Register and to ensure closer alignment to the principles of the ISO27001 information security standard.

**9.3** The Committee was informed of a cyber security incident which occurred on 9 February 2018, in which multiple false patient feedback entries were added to the Choose a Fertility Clinic section of the website. This incident impacted on 46 clinics and resulted in overall patient feedback reducing to around '2 out of 5' for many of these. The Authority was made aware of the incident on 12 February and it was investigated immediately. The false feedback added was removed within 48 hours and the affected clinics informed.

**9.4** On initial review, it appears that the feedback entries were added by an automated script by a third party unconnected to the Authority. It did not affect the underlying IT infrastructure or appear to introduce any malicious code. No clinical information was present or accessed and no data breach occurred.

**9.5** The Committee considered this to be a serious incident, questioning why technology could not prevent this happening and querying the controls in place. The Director of Compliance and information stated that the Choose a Fertility Clinic facility was initially designed for ease of use, so as to encourage engagement and feedback. However, since this incident and following a review of risk, a CAPTCHA validation check has been introduced to prevent a reoccurrence of this type of incident.

**9.6** The DHSC stated that the Authority acted swiftly in response to this incident. It was confirmed the all 46 clinics affected had been written to and no negative feedback had been received.

**9.7** The Chair thanked the Executive for their rapid handling of this incident.

## 10. Strategic Risk Register

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

**10.2** The Committee was informed that the residual risk in relation to financial viability had been reduced, due to the forecasted surplus against budget. The Corporate Management Group had felt it was too soon to reduce the residual risk level of the capability risk, as it was unclear whether mitigations had yet materially reduced the risk.

**10.3** The Chair stated that, given the conversations which had occurred at this Committee meeting, particularly about finance risk, some of the information on the risk register now seemed outdated. The Chief Executive confirmed that the timing of the review of the register by the Committee was the reason it appeared out of date in places. The Chair also stated that the section addressing mitochondrial applications may require updating.

**10.4** The Chief Executive stated that, despite the recent patient feedback incident on the website, he felt reassured that the residual risk rating for cyber security remains correct.

### Action

**10.5** The Risk and Business Planning Manager and Head of Planning and Governance to ensure the information concerning mitochondrial applications is correct in the strategic risk register, and that the financial risk is reviewed again in the near future.

## 11. AGC Forward Plan

**11.1** The Head of Finance stated that, as agreed earlier in the meeting, the ‘estates’ theme would be added to the Forward Plan.

**11.2** The Head of Finance suggested the addition of a bi-annual HR report to the Forward Planner, with a particular emphasis on the March Committee meeting, where the report should mirror information required for the Annual Report and Accounts.

**11.3** The Chief Executive stated that the Committee could be given more frequent exposure to wider HR issues, including pay ratios and the staff survey.

**11.4** The Committee agreed that a bi-annual HR report should be added to the Forward Planner, with the first report being received at the 12 June 2018 meeting.

### Action

**11.5** A bi-annual HR report to be added to the Forward Planner, with the first report being received at the 12 June 2018 meeting.

## 12. Whistle Blowing and Fraud

**12.1** The Director of Finance and Resources informed the Committee that the investigation into an alleged fraud, in connection with a contract provider, had concluded. The individual concerned did not cooperate with the investigation and had now resigned from his position at the Authority. There are no financial implications in light of the individual's resignation, apart from those associated with pension and annual leave owed.

**12.2** The Committee noted that settlement negotiations with the contract provider are ongoing. The settlement sought by the contract provider was £50k, but the question of who is liable to pay this sum has not yet been established.

**12.3** The DHSC case was proceeding and the Committee would be updated once this is concluded.

**12.4** The Committee noted the potential risk of legal proceedings against the Authority in relation to this matter.

### Action

**12.5** The Director of Finance and Resources to update the Committee on the outcome of the DHSC criminal prosecution and agreed settlement with the contractual provider in due course.

## 13. Contracts and Procurement

**13.1** The Head of Finance reported there had been one new contract at the value of £35K.

## 14. Review of AGC activities & effectiveness, terms of reference

**14.1** The Committee Members discussed this item in a private session.

## 15. Any Other Business

**15.1** Members and auditors retired for their confidential session.

**15.2** The next meeting will be held on Tuesday, 12 June 2018 at 10am.

## 16. Chair's signature

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

**Signature**

## Name

Margaret Gilmore

## Date

12 June 2018

# Audit and Governance Committee Paper

| | |
|---|---|
| **Paper Title:** | **Matters arising from previous AGC meetings** |
| **Paper Number:** | **[AGC (12/06/2018) 601 MA]** |
| **Meeting Date:** | 12 June 2018 |
| **Agenda Item:** | **3** |
| **Author:** | Morounke Akingbola, Head of Finance |
| **For information or decision?** | Information |
| **Recommendation to the Committee:** | To note and comment on the updates shown for each item. |
| **Evaluation** | To be updated and reviewed at each AGC. |

Numerically:

- 12 items added from March 2018 meeting, 3 ongoing
- 4 items carried over from earlier meetings, 4 ongoing

| ACTION | RESPONSIBILITY | DUE DATE | PROGRESS TO DATE |
|---|---|---|---|
| **Matters Arising from Audit and Governance Committee – actions from 13 June 2017 meeting** | | | |
| **15.2** The Director of Finance and Resources to ensure the Committee remains updated with regards to the outcome of the investigation | Director of Finance and Resources | | **Ongoing** - An update will be provided at the June 2018 meeting |
| **Matters Arising from Audit and Governance Committee – actions from 3 October 2017 meeting** | | | |
| **6.6** The Director of Finance and Resources to create a training plan for the Committee, ensuring sessions are scheduled to occur on the same dates as planned meetings. | Director of Finance and Resources | | **Ongoing -** An update will be provided at the June 2018 meeting |
| **Matters Arising from Audit and Governance Committee – actions from 5 December 2017 meeting** | | | |
| **4.18** The Director of Compliance and Information to provide the Committee with an update on regulatory and Register management in due course. | Director of Compliance and Information | | **Ongoing** |
| **12.8** The Director of Finance and Resources to arrange training for members to follow the 6 March 2018 meeting. | Director of Finance and Resources | | **Ongoing** – It was agreed at the March meeting this would be deferred to the Autumn meeting.<br><br>An update will be provided at the June 2018 meeting |

| Matters Arising from Audit and Governance Committee – actions from 6 March 2018 meeting | | | |
|---|---|---|---|
| **3.7** The Chief Information Officer to ensure the Committee receive periodic reviews on the position, regarding staff completion of cyber security training, particularly at times of high staff | Chief Information Officer | | **Ongoing** |
| **3.8** The Head of Planning and Governance to reissue the cyber security training link to Authority members. | Head of Planning and Governance | | An email has been sent to Authority members. |
| **3.9** The Director of Finance and Resources to liaise with the NAO regarding training to Committee members, providing an overview of the NAO work programme and their perspective on the challenges facing the NHS. | Director of Finance and Resources | | **Ongoing** - An update will be provided at the June 2018 meeting *Feedback on audit reviews/outcomes from other regulatory bodies and incorporate into agendas instead of training sessions?* |
| **4.18** The Director of Finance and Resources to add an item on estates to the Forward Plan, for regular discussion at Committee meetings, from the end of 2018. | Director of Finance and Resources | | This item has been added to the Forward Plan |
| **5.15** The Director of Finance and Resources to inform the Committee should any risks related to GDPR compliance materialise. | Director of Finance and Resources | | See below |

| | | | |
|---|---|---|---|
| **5.16** The Director of Finance and Resources would provide the Committee with an update report in mid-April 2018 and arrange a teleconference, if required, a week prior to the GDPR go live date. | Director of Finance and Resources | | The Committee were provided with an email update on 4 May 2018. |
| **5.17** The Head of Internal Audit to ensure that contractual risk is a focus point for the 2018/2019 audit programme. | Head of Internal Audit | | Plan for 18/19 includes Anti-Fraud Controls audit in Q4 2018/19 |
| **5.19** The Head of Internal Audit to conduct a review of the evidence submitted on closed recommendations, and provide confirmation to the Committee by email, if satisfied. | Head of Internal Audit | | Evidence submitted and accepted – all three closed 07/03/2018 |
| **8.15** The Committee to be kept informed of developments regarding capital requested from the DHSC and the response obtained. | Chief Information Officer | | DHSC finance approved Admin and noted capital requirement. Looks reasonably positive. |
| **10.5** The Risk and Business Planning Manager and Head of Planning and Governance to ensure the information concerning mitochondrial applications is correct in the strategic risk register, and that the financial risk is reviewed again in the near future. | Risk and Business Planning Manager/Head of Planning and Governance | | The financial risk has been reviewed, with more detail added. Information on mitochondrial applications is correct as confirmed by Head of Planning and Governance. |

| | | | |
|---|---|---|---|
| **11.5** A bi-annual HR report to be added to the Forward Planner, with the first report being received at the 12 June 2018 meeting. | Head of Finance | | This item has been added to the Forward Planner |
| **12.5** The Director of Finance and Resources to update the Committee on the outcome of the DHSC criminal prosecution and agreed settlement with the contractual provider in due course | Director of Finance and Resources | | **Ongoing** – We have accrued for a non-contractual payment in the 17/18 accounts.<br><br>An further update will be provided at the June 2018 meeting. |

# Audit and Governance Committee

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

| **Details:** | |
|---|---|
| Meeting | Audit & Governance Committee |
| Agenda items | 4a and 4b |
| Paper number | AGC (12/06/2018) 602/603 |
| Meeting date | 12 June 2018 |
| Author | Jeremy Nolan |

| **Output:** | |
|---|---|
| For information | To provide an update to the Audit and Governance Committee on our annual opinion for 2017/18 and the draft 2018/19 Internal Audit plan for approval. |
| Progress Update | **Annual Opinion for 2017/18**<br><br>1. The Head of Internal Audit's Annual Opinion for 2017/18 is at Annex A. The opinion outlines the internal audit work completed in 2017/18 and gives a 'moderate' level of assurance to the Accounting Officer that the Human Fertilisation and Embryology Authority has had adequate and effective systems of control, governance and risk management in place for 2017/18.<br><br>**18/19 Audit Plan**<br>2. The draft Internal Audit plan for 2018/19 is at Annex B. A financial budget for this work has now been agreed.<br>**Action required**<br><br>3. Members are requested to note the 2017/18 annual opinion and approve the proposed 2018/19 audit plan. |
| Actions from previous meeting | None |
| Organisational risk | ☐ Low ☒ Medium ☐ High |
| Annexes | Annex A – Head of Internal Audit's Annual Opinion for 2017/18<br>Annex B - The draft Internal Audit Plan for 2018/19 |

# ANNUAL ASSURANCE REPORT 2017/18

# *Human Fertilisation and Embryology Authority (HFEA)*

Government Internal Audit Agency

**Background**

In order to be able to provide an annual opinion for 2017/18 to HFEA's Accounting Officer, it is necessary to consider the work undertaken by Internal Audit over the course of that year, the outcomes of that work and feedback from management on improvements to their areas of responsibility as a result of that work. This together with wider intelligence gathered from other sources of assurance, and performance reporting, inform the Head of Internal Audit's view of controls, governance and risk management. This report provides an overall summary of Internal Audit work delivered in 2017/18 as well as including the formal annual opinion of the Head of Internal Audit.

**Introduction**

The Health Group Internal Audit Service (HGIAS) plays a central role in the Department of Health & Social Care and its Arms Length Bodies' (ALBs) overall governance arrangements, not least through its review of the effectiveness of risk management, the application of financial and other controls, and governance. In operating as a shared service and providing the audit service to the HFEA, HGIAS:

a. Focuses its audit activity on the HFEA's identification and management of key business risks, especially in relation to principal systems and processes;
b. Provides guidance to the HFEA Audit and Governance Committee members, managers and staff with regard to improvement and application of best practice in internal control; and
c. Provides advice to management on the internal control implications of proposed and emerging changes.

HGIAS auditors operate in accordance with Public Sector Internal Audit Standards and work to an annual Internal Audit Plan which is agreed with senior management and the HFEA Audit and Governance Committee (AGC). The Head of Internal Audit also provides an update to each meeting of the HFEA Audit and Governance Committee, which supports the Committee in the exercise of its functions.

**Compliance with Public Sector Internal Audit Standards and Quality Assurance**

Health Group Internal Audit Services (HGIAS) was subject to an External Quality Assessment (EQA) of its services in March 2016. This is a requirement of HM Treasury which should be undertaken at least every 5 years. The conclusion of an EQA can lead to one of three assessment opinions in relation to the above standards – Fully Conforms (FC), Generally Conforms (GC) and Partially Conforms (PC). The HM Treasury standard requirement for compliance is "Generally Conforms". HGIAS has been rated as Generally Conforms.

During 2017-18, HGIAS has conducted continuous quality assessments against these requirements, which indicate that our Internal Audit arrangements continue to comply with the standards and are generally satisfactory. We have strengthened our quality assurance processes in cases where audit work is provided by an outsourced supplier in order to improve both consistency across HGIAS and the service provided to our customers. Since joining the Government Internal Audit Agency in October 2016, HGIAS has participated in all assurance exercises mandated by the senior management of the Agency.

Continuous improvement in quality and consistency will continue to be a priority across the health shared service, as will the application of GIAA best practice.

**Internal Audit Work Delivered - 2017/18 Performance Summary**

| | |
|---|---|
| **Reviews carried over from 2016/17 plan** | **0** |
| | |
| **2017/2018 Agreed Programme** | **4** |
| **Total Reviews Deferred to complete in 2018/19** | **0** |
| **Total Reviews Dropped in 2017/18** | **0** |
| **Total to deliver 2017/18** | **4** |
| **Total remaining on plan to carry forward to complete in 2018/19** | **0** |
| **% of programme completed** | **100%** |

**Summary of Internal Audit Reports for 2017/18 showing Status, Outcome and Recommendations Made**

| | Audit Title | Status | Report Rating | Recommendations agreed by priority | | |
|---|---|---|---|---|---|---|
| | | | | High | Medium | Low |
| 1 | Data Loss | Final Report | Moderate | 0 | 4 | 0 |
| 2 | Risk Management [including Governance Element] | Final Report | Moderate | 0 | 2 | 0 |
| 3 | General Data Protection Regulation Preparedness | Final Report | N/A – Advisory Review | N/A | N/A | N/A |
| 4 | Financial Controls | Final Report | Substantial | 0 | 0 | 0 |
| | Recommendations Follow Up | Completed | N/A | N/A | N/A | N/A |
| | | | Total | 0 | 6 | 0 |

All the recommendations made in 2017/18 were accepted by management, who have developed action plans to further improve risk management, governance and control.

**Internal Audit Work Delivered – Rating Used**

We used the following levels of rating (in line with the agreed definitions across all government departments) when providing our internal audit report opinions:

| Rating | Definition |
|---|---|
| **Substantial** | In my opinion, the framework of governance, risk management and control is adequate and effective. |
| **Moderate** | In my opinion, some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control. |
| **Limited** | In my opinion, there are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective. |
| **Unsatisfactory** | In my opinion, there are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail. |

Internal audit now review follow-up actions for recommendations graded 'high' and 'medium'. Once HFEA has indicated that a recommendation has been implemented, we provide confirmation. Evidence has been provided to confirm that the remaining 2015/16 and 2016/17 recommendations have been implemented, and they were closed on this basis. Follow up work relating to recommendations made in 2017/18 is ongoing.

**Head of Internal Audit Opinion 2016/17**

In accordance with the requirements of the UK Public Sector Internal Audit Standards, I am required to provide the Accounting Officer with my annual opinion of the overall adequacy and effectiveness of the organisation's risk management, control and governance processes.

My opinion is based on the outcomes of the work that Internal Audit has conducted throughout the course of the reporting year and on follow-up action from Internal Audits conducted in the previous reporting year. There have been no undue limitations on the scope of Internal Audit work and the appropriate level of resource has been in place to enable the function to satisfactorily complete the work planned.

For the three areas on which I must report, I have concluded the following:

- In the case of **risk management: moderate**

  We completed a review of Risk Management during the 2017/18 financial year, which resulted in a moderate assurance rating. Two recommendations were made to enhance the quality of strategic risk register and improve the systems for identifying reasons for staff turnover. In addition, we reviewed the risk management arrangements in place with respect to Data Losses. Four recommendations were made to improve current working practices and help reduce the potential risk to HFEA.

- In the case of **governance: moderate**

  During 2017/18 we looked at elements of Corporate Governance in HFEA as part of the Risk Management review and found the risk governance structures to be strong. The only relevant recommendation made related to strengthening of the strategic risk register. We also reviewed the governance arrangements in place to effectively prepare for the introduction of the General Data Protection Regulation. As this was an advisory review, it was not rated, but a number of suggestions were made on how governance arrangements over the project could be strengthened and improved to ensure that this Regulation is effectively implemented.

- In the case of **control: Moderate**

  We reviewed controls throughout the 2017/18 audit programme, which lead to two 'moderate' report ratings and one 'substantial' rating. These reports in total contain 6 'medium' graded recommendations. Our advisory report on preparations for the introduction of the General Data Protection Regulation also made a number of suggestions for strengthening processes and controls.

Therefore, in summary, my overall opinion is that I can give **moderate assurance** to the Accounting Officer that the Human Fertilisation and Embryology Authority has had adequate and effective systems of control, governance and risk management in place for the reporting year 2017/18.

*Jeremy Nolan*
Head of Internal Audit

Government
Internal Audit
Agency

Government Internal Audit Agency

# Overview

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

As Head of Internal Audit, I am responsible for:

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

This paper sets out:

- a summary of our audit strategy;
- our approach to developing the internal audit plan;
- the proposed internal audit plan for 2018/2019.

Government Internal Audit Agency

# Our Audit Strategy

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

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

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

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

We will deliver key products including:

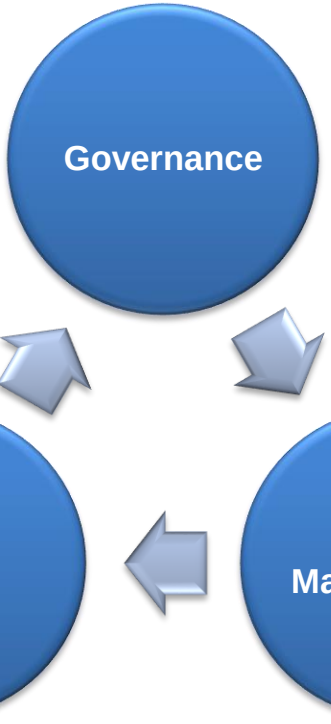
- engagement reports throughout the year, according to the timings in the plan;
- reports to each meeting of the Audit and Governance Committee (AGC) on significant risk and control issues and progress against the plan; and
- an annual assurance opinion and report.

Government Internal Audit Agency

# The Purpose of the Internal Audit Plan

The plan is designed, and will be delivered, to support an annual internal audit opinion on the adequacy and effectiveness of governance, risk management and control, through the evaluation of the extent to which:

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




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

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

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

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

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

Government Internal Audit Agency

# Our Approach to Developing the Plan

In accordance with the PSIAS, we prepared the plan on a risk basis to enable us to deliver an annual internal audit opinion and report that will conclude on the overall adequacy and effectiveness of your organisation's framework of governance, risk management and control. In preparing the plan, we considered:

**Your Objectives, Priorities and Risks**

We reviewed your objectives, priorities, strategies and targets, and assessed areas of risk to successful delivery. This included an analysis of risk information and risk registers, where available .

**Audit Universe**

We identified and assessed the key activities, systems and processes that manage areas of risk and that are critical to successful delivery of objectives. We also considered placing reliance on the work of other assurance providers to ensure proper coverage and minimise duplication of effort.

**Key Stakeholders**

We engaged widely with key stakeholders to discuss objectives, challenges and risks. Our engagement included input from Senior Responsible Officers, Directors and Executive Team members.

**Previous Internal Audit Work**

We reviewed the findings from our previous work and our knowledge and experience of your business. We have included follow up engagements in the plan where appropriate, based on findings from previous work.

Government Internal Audit Agency

# Proposed Coverage by Risk Area

| HFEA Risk Reference | HFEA Risk Category | Risk Description | Residual Risk score | Reviews |
|---|---|---|---|---|
| FV1 | Finance | **There is a risk that the HFEA has insufficient financial resources to fund its regulatory activity and strategic aims.** | 9 Medium | 1 |
| C1 | Capability | **There is a risk that the HFEA experiences unforeseen knowledge and capability gaps, threatening delivery of the strategy.** | 16 High | 0 |
| OC1 | Organisational | **There is a risk that the implementation of organisational changes results in instability, loss of capability and capacity, and delays in the delivery of the strategy.** | 9 Medium | 2 |
| CS1 | Cyber | **There is a risk that the HFEA has unsuspected system vulnerabilities that could be exploited, jeopardising sensitive information and involving significant cost to resolve.** | 6 Medium | 1 |
| LC1 | Legal | **There is a risk that the HFEA is legally challenged in such a way that resources are significantly diverted from strategic delivery.** | 12 High | 0 |
| RE1 | Regulatory | **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.** | 6 Medium | 0 |
| ME1 | Information | **There is a risk that patients and our other stakeholders do not receive the right information and guidance, so we miss opportunities to bring about positive change.** | 6 Medium | 1 |

Government Internal Audit Agency

# Summary of Plan

## Priority of engagements on the plan:

| | |
|---|---|
| High Priority: | 1 |
| Medium Priority: | 4 |
| Low Priority: | 0 |
| TOTAL | 5 |

20% of engagements are “high” priority. Completion of these would be important in order to form the basis for an evidence based assessment and robust Annual Assurance Opinion.

80% of engagements are “medium” priority. Completion of these will add value to the organisation and enhance the basis of the assessment and the Annual Opinion.

## Type of engagements on the plan:

| | |
|---|---|
| Assurance: | 5 |
| Advisory: | 0 |
| TOTAL | 0 |

100% are assurance engagements to provide an independent assessment on governance, risk management and control arrangements.

Government Internal Audit Agency

# Detailed Internal Audit Plan 2018/2019

| Audit title | Outline Scope | Audit Days | Timing | Risk Area | Risk Register Ref. |
|---|---|---|---|---|---|
| 1. Payroll and expenses | A review of how payroll and expenses are managed within HFEA, including the controls in place to ensure the accuracy and validity of payments made. **MEDIUM PRIORITY** | 8 | Q1 | Finance | FV1 |
| 2. Cyber Security | A review of the Cyber Security arrangements within HFEA, with a focus on how HFEA are compliant with the 10 steps to Cyber Security (as defined by the National Cyber Security Centre). **MEDIUM PRIORITY** | 10 | Q2 | Cyber | CS1 |
| 3. Business Continuity | This audit will be undertaken to review the Business Continuity arrangements currently operating within HFEA. **MEDIUM PRIORITY** | 10 | Q3 | Organisational | OC 1 |
| 4. General Data Protection Regulation | This will consider the extent to which HFEA are complying with the General Data Protection Regulations that will be introduced in May 2018, and will also include follow up on the 17/18 GDPR Advisory review. **HIGH PRIORITY** | 7 | Q3 | Information | ME1 |
| 5. Anti-Fraud Controls | Review of the internal controls which are currently in place within HFEA to identify, prevent and mitigate misuse of the organisations assets and/or prevent fraudulent financial reporting. This will include how these controls are managed, monitored and reported. . **MEDIUM PRIORITY** | 10 | Q4 | Organisational | OC1 |

Government Internal Audit Agency

# Detailed Internal Audit Plan 2018/2019

| Audit title | Audit Days |
|---|---|
| Head of Internal Audit and General Management | 15 |
| Contingency | 5 |
| **TOTAL** | **65** |

# Progress with Audit Recommendations

| | | | |
|---|---|---|---|
| **Strategic delivery:** | ☒ Setting standards | ☐ Increasing and informing choice | ☒ Demonstrating efficiency economy and value |
| **Details:** | | | |
| Meeting | Audit and Governance Committee | | |
| Agenda item | Progress with Audit Recommendations | | |
| Paper number | AGC (12/06/2018) 604 MA | | |
| Meeting date | 12 June 2018 | | |
| Author | Morounke Akingbola, Head of Finance | | |
| **Output:** | | | |
| For information or decision? | For information | | |
| Recommendation | The Committee is asked to Note: there are 4 audit recommendations of which 3 remain open and one of which has a due date that is later than previously planned. | | |
| Resource implications | None | | |
| Implementation date | During 2017–18 and 2018 - 19 business year | | |
| Communication(s) | Regular, range of mechanisms | | |
| Organisational risk | ☐ Low | ☒ Medium | ☐ High |

## *SUMMARY OF AUDIT RECOMMENDATIONS*

| Year of Rec. | Category | Audit | Section | Rec # | Recommendations | Action Manager | Proposed Completion Date | Complete this cycle? |
|---|---|---|---|---|---|---|---|---|
| 2017/18 | M | DH Internal Audit | Data Loss | 1 | **Clinic governance oversight** | ***Chris Hall, Senior Inspector (Information)*** | ***Post April 2018*** | No |
| | M | | | 2 | **Policy Review** | ***Dan Howard, CIO*** | ***May 2018*** | No |
| | M | | | 3 | **Staff Training** | ***(Dan Howard, CIO & Head of HR)*** | ***December 2017*** | Yes |
| | M | | Risk Management | 2 | **Staffing / Capability** | ***Peter Thompson, CEO (Yvonne Akinmodun, Head of HR)*** | ***March 2018*** | No |
| **TOTAL** | **4** | | | | | | | |

| FINDING/*RISK* | Recommendation | Management Response and agreed actions / Progress update | Owner/Completion date |
|---|---|---|---|
| **2017/18 – INTERNAL AUDIT CYCLE** | | | |
| **DATA LOSS** | | | |
| **1. Clinic governance oversight** | | | |
| The HFEA regularly inspects UK fertility clinics and research centres. This ensures that every licensed clinic or centre is adhering to standard safety. The purpose of an inspection is to assess a clinic's compliance with the Human Fertilisation and Embryology Act 1990 (as amended), licence conditions; General Directions and the provisions of the Code of Practice. The results of these audits from 2016/17 have not identified any significant weaknesses. The NAO accompany one visit per year. | The new Senior Inspector role should include responsibility over the Clinics' governance arrangements in managing data loss, including:<br>a. Clinics' information governance arrangements to mitigate the risk of data losses;<br>b. Clinics' arrangements for staff training on information management;<br>c. Clinics' BCP arrangements. | **The Senior Inspector (Information) role has been reviewed and it includes responsibilities for reviewing Information Governance. This includes staff training and security arrangements which includes reviewing BCP planning.**<br>***Inspection regime to be updated to reflect requirements within the new Senior Inspector (Information Quality) post will be filled from – Summer 2018***<br>***Nov 17 update:*** no update<br>***Feb 18 update:*** no update<br>***May 18 update:***<br>The Senior Inspector (Information Quality) will be filled from August 2018 | ***Chris Hall, Senior Inspector (Information Quality)***<br>***Summer 2018*** |
| **2. Policy Review** | | | |
| Key policies and some of the Standing Operating Procedures were not up to date and were not reviewed on a regular basis - there is a risk that the policy may be out of date and result in incorrect processes being followed. | Key data and information policies should be reviewed periodically to ensure that they are current and aligned. | **Information Access Policy and SOPs to be reviewed, updated and ratified to reflect GDPR requirements. Staff Security Procedures (Acceptable Use Policy) to also be updated**<br>***To align with GDPR legislation and to be updated as a component of the HFEA GDPR Action Plan - May 2018. Update and approve at CMG – January 2018***<br>***Nov 17 update:*** *We have established a joint project with the HTA and we are developing an overarching project plan and have started the assessment against the 'Nymity Data Privacy Accountability Scorecard'. The recruitment to the IG Project Officer is ongoing.*<br>***Feb 18 update:*** no update<br>***May 18 update***: The new Acceptable Use Policy was reviewed at CMG on 23 May 18. Final comments will be forward to DH before 6 June 18 and the final version of | ***Owner: Dan Howard, CIO***<br>**May 2018** |

| | | | |
|---|---|---|---|
| | | policy will be reviewed and ratified by CMG on 20 June 2018 | |
| **3.** | **Staff Training** | | |
| We identified that the HFEA Business Continuity Plan has not been tested on a regular basis. It was therefore not possible for HFEA to provide assurance that the BCP remains current, fit for purpose and reflects key personnel change to ensure roles and responsibilities are clear. | A process should be put in place to ensure that HFEA are able to capture and monitor all mandatory information management learning and development carried out. | **We will refresh our approach to the completion of the following modules of mandatory training in IG. Our target is that all staff will have completed these in the previous 12 months by the end of the calendar year. The modules are:**<br>• **Responsible for information: general user;**<br>• **Responsible for information: information asset owner (IAOs to complete); and**<br>• **Responsible for information: senior information risk owner (SIRO to complete)**<br>***All staff – December 2017. The framework for mandatory training (in all areas including information training requires refresh). In any event whilst many staff have undertaken training within 12 months we will use Oct-Dec period to ensure all staff have completed, with sign off from Managers.***<br><br>***Nov 17 update:*** *Information management training has been identified for all staff. Information Asset Owners, SIRO and all remaining staff will be expected to complete this before the end of December 2017.*<br><br>***Feb 18 update:*** *All staff were required to complete the online IAO training in December 2017. With HR monitoring to ensure completion.*<br><br>*HR is also in the process of purchasing a new HRIS which will enable the training, monitoring and recording of mandatory and other training provided by HFEA. It is expected the new system will be in place by early spring 2018*<br><br>***May 18 update***: The new HR system is in the process of being configured. It is expected that the new system will go live on 1 July 2018 | ***Dan Howard, CIO*** *(Yvonne Akinmodun)*<br><br>**December 2017**<br><br>**Complete** |

| 4. | Staffing / Capability | | |
|---|---|---|---|
| There is the potential that HFEA are exposed to continued high staff turnover, loss of experience and expertise, which could lead to knowledge gaps and disruption to key areas of the business, affecting the service provided. | HFEA should put in place mechanisms to ensure that information captured through exit interviews and staff surveys to identify the root causes behind staff turnover, is used effectively to implement practical changes to bring turnover levels in line with agreed tolerances. This should include, but not limited to:<br><br>•Ensuring that all information gathered from staff during exit interviews and staff surveys is reviewed in detail, with an action plan produced to respond positively to the findings. Any actions agreed should have senior management sponsorship to ensure there is the requisite accountability and a clear mandate for implementing the actions agreed; and<br><br>•Development of a clear workforce strategy which supports management in the recruitment and retention of staff. | ***A management action plan which provides details of planned actions for addressing the root cause of current staff turnover in HFEA, incorporating some or all of the elements detailed in the recommendation.***<br><br>***Agreed. We will look at this suggestion in the near future. Discussion at the next available SMT.***<br><br>***Feb 18 update:*** Review of staff survey results was conducted in Q3 by CMG and shared with staff in January.<br>Plans are currently being put in place to provide quarterly or bi-annual reports to SMT on the general themes that emerge from exit interviews. Action plans to tackle themes identified from exit interviews will also be put in place<br><br>***May 18 update:***<br>**In progress – results from the findings from exit interviews will be reported as part of an annual HR report**<br><br>***Agreed – this is in progress. Finalisation discussion planned at leadership and away day on 29 November 2017. Publication shortly thereafter.***<br><br>**Feb 18 update:** We have a people plan which identified recruitment and retention processes including the review of our induction process to ensure staff feel able to work effectively in as short a period of time as possible.<br><br>***May 18 update:***<br>**A new induction policy and checklist was launched in May 2018. Managers are being offered guidance and support in using the new policy** | ~~***Juliet Tizzard, Director of Strategy & Corporate Affairs***~~<br>~~***Paula Robinson***~~<br><br>***Peter Thompson, CEO***<br>***Yvonne Akinmodun***<br><br>***Before end of 2017***<br><br>~~***TBC***~~<br><br>***End March 2018*** |

# Digital Programme Update: June 2018

| | | | |
|---|---|---|---|
| **Strategic delivery:** | ☒ Setting standards | ☐ Increasing and informing choice | ☒ Demonstrating efficiency economy and value |
| **Details:** | | | |
| Meeting | Audit and Governance Committee | | |
| Agenda item | 9 | | |
| Paper number | AGC (12/06/2018) 610 DH | | |
| Meeting date | 12 June 2018 | | |
| Author | Dan Howard, Chief Information Officer | | |
| **Output:** | | | |
| For information or decision? | For information | | |
| Recommendation | The Committee is asked to note:<br>• Progress made on data migration, development of PRISM, release of APIs, and supplier / clinic engagement and how we will launch our new system and new register in October 2018<br>• The financial update, and<br>• Details of key risks, mitigations and contingency<br>The Committee is asked to approve:<br>• The approach for monthly updates until programme conclusion, and<br>• The approach for data migration sign-off (as outlined in section 4) | | |
| Resource implications | None | | |
| Implementation date | During 2018 - 19 | | |
| Communication(s) | Regular, range of mechanisms | | |
| Organisational risk | ☐ Low | ☒ Medium | ☐ High |
| Annexes: | None | | |

# 1. Background

**1.1.** In March 2018, AGC received a progress update on data migration and development of our new data submission system, PRISM. This included new forecasts in relation to funding the programme to completion, and the impact on capital expenditure approval this year. Since then, substantial progress has been made; data migration is nearing completion, the APIs have been launched (used by system providers to link into our new register) and system suppliers have signalled they will complete their development on time. In addition to this, PRISM development is progressing well and we are readying ourselves, clinics and suppliers for launch in October 2018. In addition, whilst capital expenditure approval is outstanding (a single approval is made by DHSC for all NHS and DHSC bodies) we are optimistic this will be granted.

**1.2.** While significant progress has been made since March, some issues have arisen during the past month. Firstly, it was necessary to update the database structure (schema) for the new register and this has had an impact on the timeline for data migration. Secondly, planning the preview (test) version of PRISM identified additional work which must be completed ahead of launch. While these have absorbed contingency (financial and time) more quickly than ideal we remain confident that the project will be delivered within the timescales we have specified and within the agreed budget.

**1.3.** This paper updates on AGC on progress, the financial forecast and risk/issues. Given the next AGC meeting is not until October 2018, it makes recommendations as regards updating AGC over the next three (crucial – in terms of delivery) months. More specifically it also proposes an approach for the final approval by AGC for data migration to take place, once all validation checks have been completed.

# 2. Summary

**2.1.** **System and new register launch:** We remain on track for full launch of the working system for all clinics in October 2018 as signalled in the previous update in March 2018. As communicated at the annual conference earlier this year, the preview launch of PRISM will take place later this month. This will allow clinics and other stakeholders the opportunity to evaluate the look, feel and core functionality of the system.

**2.2.** **Data cleansing and migration:** Substantial progress has been made on the detailed work associated with data migration and data cleansing. While the schema changes resulted in a small delay to data migration, we are still confident this work will complete to the quality we expect, and will not delay go live in October. The data dictionary has been completed and launched. The database schema is now stable and settled, giving the basis for much improved clarity and understanding of the new Register. We are in the final two data migration tasks of mapping data to allow it to be transformed into the Register schema, maintaining the data quality we currently expect.

**2.3.** **'PRISM' system development:** The majority of PRISM has now been developed and with some work continuing on the final stages. Many APIs, the code to enable third-party clinic system suppliers, have been launched and we have had good engagement with suppliers and they have indicated their ability to meet the timetable.

**2.4.** **Transitional Arrangements:** Our transitional arrangements are progressing well. We have been communicating regularly with clinics and EPRS providers and this has been well received. We have discussed our plans for go-live – and the requirement for system suppliers to update their systems to align to the new register – and we have received a positive response. We will continue to monitor to suppliers during the summer to ensure they are ready for launch.

**2.5.** **Cloud environment:** The cloud infrastructure to host the new Register has been built. Detailed and comprehensive penetration testing (phase 1 of 3) has taken place, the results of which were very positive and did not identify any unexpected issues.

**2.6.** **Risk and issues:** A significant degree of risk continues to be monitored and several significant risks remain relating to complexity, timeline, availability of key staff and reliance on those external to the project (EPRS providers).

Two issues have recently arisen:

- On testing the data migration transfer load process following changes to the schema, it became apparent that there was more work needed beyond that introduced by the schema changes. Re-planning the work allocates our contingency (both in terms of time and resource). The plan takes data migration until the end of September, but still allows us to go-live in October.
- Planning the release of PRISM (preview) identified tasks that had been set aside, but needed to be completed. In addition, testing some assumptions identified the scale of work for the remaining tasks was greater than planned.

**2.7.** **Financial:** In line with the financial forecast provided to AGC in March 18, we requested capital cover from DHSC of £500k for 18/19. While this level of cover has not yet formally been approved by DHSC, verbal assurances have been very positive and we understand that final approval is reliant on Ministerial sign off of the overall DHSC Capital programme.

## 3. Programme Plan update

**3.1.** Since the previous update in March 2018, our plans for system and register launch have progressed significantly. As signalled in March 2018, we have a single go-live scheduled for the PRISM system and APIs in October 2018. This allows time for the preview version (due for launch later in June) to be evaluated throughout the summer. It also allows time for EPRS providers to upgrade their systems to work with the APIs.

**3.2.** The programme plan remains on track to see all pre-transition work to be complete by the end of August, switch off the legacy system and cut-over to the new register during September, with the new register fully live during October. The summary programme plan is available as Annex 1.

Several milestones remain:

- The PRISM system will be made available to clinics for familiarisation (in preview form) during June 2018.
- Data Synchronisation completed – June 2018
- Data Migration - load process and validation/verification – August 2018
- Suppliers to have switched over their clinics to the new system - September 2018

- The legacy register will be switched off, final data migration will take place and transition and deployment of the system will take place thereafter - September 2018
- Data submissions via PRISM and the EPRS API enabled - September 2018.

**3.3.** Communications and engagement continue, with regular and continual engagement with clinics, third party system providers, and other stakeholders such as NHS Digital. We have signalled to EPRS suppliers – and clinics - that we expect to take a firm but fair line and suppliers will be given a reasonable timeline by which to update and deploy their systems to align to our new dataset. For any who are unable to do this, the default position for clinics is that they will need to use the PRISM system to submit data to us. All feedback from EPRS suppliers has been positive.

**3.4.** Given the nature of a system of this type, there will be a requirement for continual improvement relating to the new Register and PRISM system. Future development requests after go-live will be reviewed and prioritised by our IT Development Programme Board. Post go-live we will also commence an internal programme of data quality improvements, aligned to our strategy.

## 4. Future updates and data migration approval by AGC

**4.1.** We are keen to ensure that AGC receives regular updates on this programme as it concludes. Given the next AGC meeting is in October 2018 it is suggested that AGC receive written monthly updates on progress, highlighting any adverse variances against the programme plan or increased risk.

**4.2.** Data migration will take place only when we are confident that the validation, verification and load processes meet the acceptable quality threshold. Our assumption is that AGC will wish to have the opportunity to have detailed sight of the assurance mechanisms we have put in place to 'sign off' data migration ahead of the transfer from the current register into the new Register.

**4.3.** Should any significant issues arise between now and launch we propose facilitating a meeting between the Chair (AGC), Chief Executive, Director of Compliance and Information and Chief Information Officer to discuss the exception report. We also propose that this group provides the approval to proceed with data migration supported by a paper to all board members for comment.

## 5. Risk Management

**5.1.** Several significant risks remain to delivery of this programme; these include:

- **Loss of key staff**: The programme is heavily dependent upon a few key staff. The loss of any one could have a severe impact on the plan and quality of deliverables, depending the timing of departure. This risk has materialised with the resignation of the Register Information Team Manager at the end of May, who will depart at the end of August. This will happen after the completion of the Data Migration Load process and development of PRISM. While this presents a project issue following her departure during transition to go-live, it provides a longer term opportunity to revisit and refresh our data quality vision and consider how this can be best achieved.

Recruitment to this position has commenced. This risk carries a post mitigation score of 15.

- **The complexity of data migration** unforeseen issues emerge during sprints, risking slippage to the project and overall programme. This risk continues, although as we approach the end of the project the risk of such unforeseen issues must reduce, and we still remain on track for go-live in October. We continue to keep close track of the plan to ensure we are aware of any issues and these can be addressed. This risk carries a post mitigation score of 15.
- **Pace of Delivery:** The programme needs to deliver at pace for a further five months. Key staff have been working on the project for three years already and risk burnout. Our mitigation is careful management of time and demands on key staff members. This risk carries a post mitigation score of 10
- **RITA development (internal data review system for data interrogation) takes longer than expected delaying the roll out**: We are developing using a 'Waterfall' rather than 'Agile' project management methodology. This will entail detailed up front design, but give clarity to timeframes. A minimum RITA requirement (Release 1) for go live has been specified and will be developed first. Future development requests will be reviewed and prioritised by the IT Development Programme Board and the Corporate Management Group and we expect an iterative development over time, aligned to our organisational objectives. This risk carries a post mitigation score of 15.

**5.2.** The full risk register is available on request.

## 6. Financial

**6.1.** The programme is delivering on target, and within the £500k capital cover that we expect to be approved shortly by DHSC.

**6.2.** Given the impact of the schema changes and additional PRISM development, we are reprofiling the project to remove several components of RITA functionality and reduce the amount of performance testing we undertake. This will ensure the project delivers on target and within the financial envelope we have agreed.

## 7. Recommendation

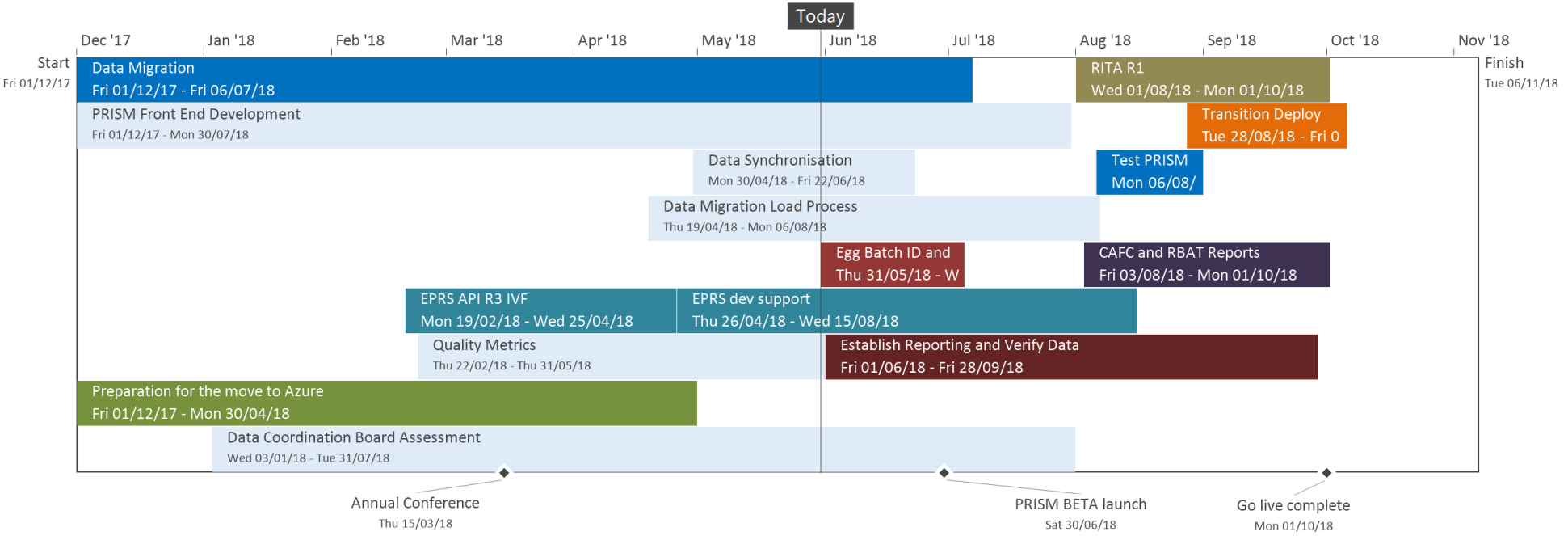
The Committee is asked to note:

- Progress made on data migration, development of PRISM, release of APIs, and supplier / clinic engagement and how we will launch our new system and new register in October 2018
- The financial update, and
- Details of key risks, mitigations and contingency

The Committee is asked to approve:

- The approach for monthly updates until programme conclusion, and
- The approach for data migration sign-off (as outlined in section 4)

# 8. Annexe 1: Summary Programme Plan



# Resilience, Business Continuity Management and Cyber Security

| | | | |
|---|---|---|---|
| **Strategic delivery:** | ☒ Setting standards | ☐ Increasing and informing choice | ☒ Demonstrating efficiency economy and value |
| **Details:** | | | |
| Meeting | Audit and Governance Committee | | |
| Agenda item | 10 | | |
| Paper number | AGC (12/06/2018) 611 DH | | |
| Meeting date | 12 June 2018 | | |
| Author | Dan Howard, Chief Information Officer | | |
| **Output:** | | | |
| For information or decision? | For information | | |
| Recommendation | The Committee is asked to note:<br>• The penetration test results relating to the new server environment created for the new register<br>• Details of a server incident in April affecting core system access<br>• Server infrastructure and support and details of our programme of transformational work migrating server services into the Microsoft Azure 'cloud' | | |
| Resource implications | None | | |
| 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.** This paper provides an update on the results of penetration testing on the new register infrastructure, details of a recent server incident and provides an update on our programme of work to migrate services from physical servers to the Microsoft Azure cloud, in line with our IT strategy, resulting in improved resilience, security and system availability.

**1.3.** Penetration testing (phase 1 of 3) has been completed on the new Register infrastructure and the results are below. As can be seen, the results were very positive and did not identify any unexpected issues.

**1.4.** We experienced a server incident resulting in unavailability of Epicentre (our licensing database) and our Register during April. An overview of the incident, immediate action taken and lessons learnt following the incident are summarised below.

**1.5.** This paper includes a summary of our arrangements for server infrastructure support. We have entered into a six-month contract for infrastructure support and the completion of associated transformational projects to migrate services from physical services in Spring Gardens to Microsoft Azure (known as 'the cloud').

# 2. Penetration testing

**2.1.** Penetration testing for the main PRISM infrastructure, additional internal facing servers and application servers is underway in line with our programme plan. It is broken down into discrete phases, as follows:

- Phase 1: Relating to PRISM infrastructure – testing completed in May.
- Phase 2: Relates to the application penetration test along with three additional new internal servers yet to be built. The second test is reliant on completion of the programme of data synchronisation work. The second penetration test take place during the second half of June.
- Phase 3: Relates to a final applications and infrastructure test and this will be completed once RITA development (internal system) is complete. This test will be completed in September.

**2.2.** The results of phase 1, are within Annex 1. There we no significant risks identified.

**2.3.** We have carefully reviewed the findings with Alscient and our CLAS consultant (security advisor) and we have been in regular contact with NTA who undertook this assessment. NTA have agreed our response for each of the findings is reasonable, proportionate and appropriate.

**2.4.** As our penetration testing programme is undertaken we will regularly report back on progress, findings and action taken.

## 3. Server incident

**3.1.** On 18 April 2018 at around 4pm we encountered an issue with data access on one of our servers in Spring Gardens. The evidence at the time pointed to the root cause being a hard drive failure affecting access to three files which are part of a nine file set relating to application data and database data last updated on 18 April. The initial investigation suggested it could be related to corrupt files, a physical hardware issue, a software issue relating to file access or a software issue relating to the management of the hardware (firmware).

**3.2.** This was discovered on 18 April at around 4pm. While we took immediate action, by the following morning several IT services were affected including TRIM, Skype, desk phones, Pulse, Epicentre, Outlook (for some users) and EDI.

**3.3.** At the time evidence suggested the most likely reason for the issue was a damaged hard drive within the server. A replacement drive was procured while further work continued to restore the (current, 18 April) set of files.

**3.4.** Detailed and systematic work was undertaken at the time to stabilise as many IT systems as possible. Following our initial work, although there was some turbulence during recovery, the majority of services highlighted above were re-established very quickly enabling the majority of staff to work as normal. Following this work, Epicentre and the QA app (used internally) was still unavailable and clinics were unable to submit treatment data to us.

**3.5.** Four separate pieces of recovery work were started and managed in parallel:

1) We copied the 18 April version (most recent) of application and database (register) data from storage within our physical server to separate ‘network’ storage. This would then need to be compressed, uncompressed and restored. Further analysis of this snapshot of data took place.
2) We investigated and then decided against taking a new backup from the 18 April version of application and database data. This decision was taken because this was a live (albeit unfunctional) environment and this action carried an unnecessary level of risk.
3) We engaged a third party data recovery specialist to investigate the 18 April version of the file set to look at repairing the data so that it (or as much as possible) could be recovered. The suite of files is over 1 Terabyte which is extremely large.
4) We engaged hardware specialists relating to the physical infrastructure we have (Dell EMC). They may be able to provide specialist guidance on restoration of the 18 April version of the files. We will need to engage in a support contract, update the server software which manages the hardware (firmware) and resources will need to be scheduled to support us.

**3.6.** Following work on option 1 above, we merged data from a previous register backup from 8 April and from the database tables from the 18 April backup. Following this very detailed work, access was restored to the QA app, and EDI was functional again on 8 May. Access was restored to Epicentre on 14 May.

**3.7.** During the outage we regularly updated staff and clinics – and this was well received.

## 4. Server infrastructure, support and business dependency

**4.1.** The incident referenced in paragraph 3 underlined the importance of taking the decision to improve the resilience of our server infrastructure earlier this year. In March 2018, CMG approved an approach for a six-month contract for infrastructure support and improvement to be commissioned with a third party IT provider. This is now in place with an established and proven provider, Alscient.

**4.2.** Our IT strategy is 'cloud first' providing resilience, stability and enabling us to adopt 'best of breed' technology choices. Our Office 365 environment containing OneDrive data storage and email is already held within Microsoft Azure.

**4.3.** We have commenced a programme of work to deliver more of our infrastructure into the Microsoft Azure cloud and therefore ensure greater resilience. We are directly managing some projects and supporting others. Details are as follows:

- **PRISM, inc new Register, HR system, Intranet:** New systems have been commissioned and will be hosted within the Microsoft Azure 'cloud'
- **Skype/Teams, Telephones, Sage/WAP:** Currently hosted on physical servers within Spring Gardens. Will be migrated by September 2018
- **TRIM:** Currently hosted on physical servers within Spring Gardens. Work underway to identify and implement replacement document management system
- **Epicentre inc Risk Tool and other minor internal systems:** Will remain on physical infrastructure at end 2018. We expect to review Epicentre during 2019/2020 financial year.

**4.4.** Following the incident in April/May 2018 we have also agreed a programme of specific improvements. These are technical in nature and description and are included here for the record. These include:

- Separate backups onto two separate storage locations and separate Veaam and SQL (significant server services) backups.
- Update firmware software – this is the software which manages the server hardware
- Continue root cause analysis on current issue
- Ensure we have adequate support in place - completed
- Test to ensure patching regime is appropriate for the VMWare server
- Investigate alternative ways of backing up to the cloud via an automated script
- Test the connectivity to the Storage Area Network (SAN)
- Eliminate issues with DHCP configuration – this action relates to improvements in the way in which devices are allocated unique network addresses so they can function correctly
- Move domain controllers to a more up-to-date version, possibly 2016. Domain controllers are devices on a network which manage and respond to requests for logon or to access network resources
- Rationalise the Active Directory structure and consider moving into Azure. Active Directory manages security and distributes resources.

**4.5.** The expectation is that by early 2019 the majority of IT services at HFEA will be hosted in Azure.

**4.6.** By early 2019 the major IT system left on premise will be Epicentre. Migration may not be possible to Azure given the age of the system. Work is underway to consider the hosting options for Epicentre.

**4.7.** There is a very remote chance that an incident may affect the single Microsoft Azure location where HFEA services are located. Work is underway to safeguard against this extremely unlikely eventuality occurring by mirroring our Azure services and environment – having an active copy of our data and environment elsewhere within 'the cloud'.

## 5. Recommendation

The Committee is asked to note:

- The penetration test results relating to 'phase 1' and the new server environment created for the new register
- Details of a server incident in April affecting system access
- The server infrastructure and support along with details of our programme of work to migrate server services into the Microsoft Azure 'cloud' thereby enhancing our resilience.

# 6. Annex 1: Penetration test results

| Ref | Item | Review, and action taken |
|---|---|---|
| CVE-2014-8730 | Transport Layer Security (TLS) version | TLS is the server service which encrypts data in transit.<br>Recommendation that the version of TLS is upgraded from 1.0 to 1.2. This relates to internal facing servers only as all external resources are on TLS1.2. The affected servers are: r2-management, r2-siqlog, r2-web1, and r2-web2<br>This could only be exploited by someone who had already gained access to the internal network. We have agreed with NTA (penetration test auditor) given the low level of risk, we will accept this risk. No further action to be taken at this stage. |
| CVE-2015-2808 | Cipher Suites – use of RC4 | Cipher suites are a set of algorithms which help a secure network connect use the TLS server service which encrypts data in transit.<br>Recommendation that we upgrade to TLS1.2 thus removing the requirement of using RC4. Cipher suites may introduce a very small number of biases when creating the random stream while encrypting. The use of cipher suites may decrease the randomness of encryption.<br>See TLS action above – given this affects those who have gained access to the network and the very low level of commensurate risk, we have agreed to accept this risk for the time being. No further action to be taken at this stage. |
| SVC-331 | Web component identified | A very low level risk. We have agreed to accept this risk for the time being. No further action to be taken at this stage. |
| SVC-675 | Verify SSL servers as trusted | SSL is the standard security technology for establishing an encrypted link between a web server and an internet browser (used for accessing systems or data).<br>Security certificates are only used for internal communications. Removing this risk will require significant work to install and maintain security certificates for all client devices and would introduce a new dependency which may cause operational issues with clinics accessing PRISM.<br>We have discussed this risk with NTA and have jointly concluded that the operational overhead in addressing the risk, outweighs the security risk and on that basis we will accept this risk, but we will routinely monitor our approach as technology develops. No further action to be taken at this stage. |
| SVC-1393 | Cipher Suite strength | As with CVE-2015-2808. This applies only to internal servers. We have agreed to accept this risk for the time being. No further action to be taken at this stage. |
| SVC-264 | HTTP options | This risk relates to the way in which client devices communicate with our server infrastructure. This is a low risk and is by design. The websites need to support the HTTP options to provide the necessary functionality. No further action to be taken at this stage. |

| | | |
|---|---|---|
| ASA-702 | Admin password strength | Recommendation to update the admin password complexity to improve security controls and reduce the risk of systems being compromised. Action agreed and password strength will be improved. To be completed by end July 2018. |
| ASA-712 | Admin password sharing | Different usernames and passwords are used on the gateways. Only the internal ones are similar. Implementing different passwords on all servers creates an operational risk as they are likely to be forgotten and a security risk given there will be so many they are likely to be recorded (albeit within a secure encrypted password 'vault'). Having considered this risk we feel this is the appropriate balance and no further action to be taken at this stage. |
| ASA-886 | Password policy | The general password policy (in terms of frequency of changing and password complexity) should be updated. Action agreed and this will be completed by end July 18. |
| ASA-1339 | SMB signing | SMB Signing is a feature through which communications using SMB (Secure Message Block) can be digitally signed at the packet level. A packet of data is a unit of data transferred across a network.<br>This only applies on internal servers and so this risk is very similar to CVE-2014-8730 and CVE-2015-2808. we have agreed to accept this risk for the time being. No further action to be taken at this stage. |
| Patch management | | The risk relates to ensuring our infrastructure is appropriately patched. The patches listed in the report are all redundant or have been superseded with newer patches which have been applied. No further action to be taken at this stage. |

# 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 | 11 |
| Paper number | HFEA (12/06/2018) 612 HC |
| Meeting date | 12 June 2018 |
| 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.<br><br>SMT review the strategic risk register monthly.<br>AGC reviews the strategic risk register at every meeting.<br>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. Changes in risk management approach

**1.1.** During its annual review in February, the Corporate Management Group (CMG) discussed how it addressed risk management through quarterly risk meetings. In March, CMG decided to cease holding this separate quarterly risk meeting and agreed to defer detailed reviews of the strategic risk register to the Senior Management Team (SMT). This allows Directors to formally consider the register at more frequent, monthly intervals and for Heads to focus upon the operational handling of risks and identifying emerging risk sources.

**1.2.** Heads are still involved in revising the strategic risk register, giving updates on actions and Directors engage with their management teams on both operational and strategic risk on a regular basis.

**1.3.** We are in the process of formally revising the risk policy and processes to reflect these changes, along with including changes relevant to the General Data Protection Regulations. These changes will be signed off by CMG and the risk policy will come to the Audit and Governance Committee for your information in October.

## 2. Latest reviews

**2.1.** The Authority received the risk register at its 9 May meeting.

**2.2.** SMT reviewed the strategic risk register at its meeting on 29 May. SMT reviewed all risks, controls and scores.

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

**2.4.** One of the six risks is above tolerance, CS1, Cyber Security.

## 3. Recommendation

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

Latest review date – 29/05/2018

# Strategic risk register 2017/18

## Risk summary: high to low residual risks

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

* Strategic objectives 2017-2020:

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

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

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

Consistent outcomes and support: Improve access to treatment

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

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

** This column tracks the four most recent reviews by AGC, CMG, SMT or the Authority (eg,⇧⇔⇩⇔).
**Note**: as of April 2018, SMT review the strategic risk register rather than CMG. It is circulated to CMG afterwards.
Recent review points are: AGC 6 March⇨SMT 16 April⇨ Authority 9 May⇨SMT 29 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 | **2** | **3** | **6 - Medium** |
| **Tolerance threshold:** | | | | | **9 - Medium** |

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

| Commentary |
|---|
| **Below tolerance.**<br>In February CMG reduced this risk, owing to the newly implemented forecasting model and the near certain likelihood of a surplus, this brought it below tolerance. Shortly afterwards, it became clear that developments in the digital projects would require an increase in capital spending in the 2018/19 budget.<br>As at May 2018 we have not yet had confirmation from DHSC of our additional capital allocation. We have sufficient capital cover to sustain activities to the end of the first quarter. We expect confirmation before the end of Q1 but should cover not be confirmed this would be a discussion for CMG, with escalation to AGC and Authority as required. Although this risk relates to the organisation's budget the key risk is to delivery of the digital projects, since we would not be able to proceed without capital cover. The risk is therefore included in greater detail under the regulatory effectiveness risk. |

| 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.<br>We have established a model for forecasting treatment fee income and this reduces the risk of significant variance, by utilising historic data and future population projections. As at May 2018, the current receipts are within 1% of the model's forecast. We will refresh this 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:<br>• it is linked directly to level of treatment activity in licensed establishments<br>• 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.<br>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<br>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 flags any shortfall or further funding requirements.<br>All project business cases are approved through CMG, so any financial consequences of approving work are discussed. | Quarterly meetings (on-going) – Morounke Akingbola<br>Ongoing – Richard Sydee |
| Inadequate decision-making leads to incorrect financial forecasting and insufficient budget. | Within the finance team there are a series of formalised checks and reviews, including root and branch analyses of financial models and calculations.<br>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<br>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.<br>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.<br>Work is planned to improve project budgeting following some very minor (less than £5,000) overspends. | Ongoing – Richard Sydee or Morounke Akingbola<br>Monthly (on-going) – Morounke Akingbola<br>Finance training for all project managers in Q2. Renewed focus on project budgeting at Programme Board – Wilhelmina Crown |

| | | |
|---|---|---|
| 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.<br>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<br>Annually and as required – Morounke Akingbola |
| Failure to secure capital cover for the remaining IfQ spend in 2018/19 | Although this risk is technically financial, the mitigations and effects are business ones affecting delivery of the planned work. If the risk were to materialise, careful consideration would be needed to assess available actions and impacts. This risk is reflected further under the regulatory effectiveness (RE1) risk. | Nick Jones/Richard Sydee |
| **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.<br>The final contingency for all our financial risks would be to seek additional cash and/or funding from the Department. | Monthly – Morounke Akingbola<br>As at May 2018 there is one litigation matter on the horizon (scheduled to be held in the high court in Autumn 2018). |
| **DHSC:** GIA funding could be reduced due to changes in Government/policy. | A good relationship with DHSC Sponsors, who are well informed about our work and our funding model. | Accountability quarterly meetings (on-going) – Richard Sydee |
| | Annual budget agreed with DHSC Finance team alongside draft business plan submission. GIA funding has been provisionally agreed through to 2020. | December/January annually – Richard Sydee |
| | We will be undertaking a review of budgets for 2018/19 as part of our business planning process. | Planned for Q4 2017/18 – Morounke Akingbola |

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

| **Inherent risk level:** | | | **Residual risk level:** | | |
|---|---|---|---|---|---|
| Likelihood | Impact | Inherent risk | **Likelihood** | **Impact** | **Residual risk** |
| 5 | 4 | 20 – Very high | **4** | **3** | **12 - High** |
| **Tolerance threshold:** | | | | | **12 - High** |

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

| Commentary |
|---|
| **At tolerance**<br>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.<br><br>Since we are a small organisation, with little intrinsic resilience, it seems prudent to retain a low tolerance level. After a period of high turnover and internal churn, in part caused by the organisational change programme, the organisation has entered a period of greater stability. As at the end of May 2018, turnover is within tolerance.<br><br>Work continues to improve the offer to staff, with the aim of increasing the likelihood of staff staying in post and developing at the HFEA, rather than leaving, although we are limited by wider government pay constraints. |

| 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.<br><br>We plan to put in place corporate guidance for all staff for handovers. A checklist for handovers has been written and this will be circulated to managers when staff leave. This checklist will reduce the risk of variable handover provision. | In place – Yvonne Akinmodun<br><br>Checklist written – to be used from Q1 when staff leave – Yvonne Akinmodun |
| | Vacancies are addressed speedily, and any needed changes to ways of working or backfill arrangements receive immediate attention.<br><br>CMG and managers prioritise work appropriately when workload peaks arise. | In place – Yvonne Akinmodun<br><br>In place – Peter Thompson |

| | | |
|---|---|---|
| Poor morale could lead to decreased effectiveness and performance failures. | Engagement by managers through team and one-to-one meetings to obtain feedback and identify actions to be taken. | In place – Peter Thompson |
| | Staff survey results for 2017/18 informed the development of the people strategy. The all staff awayday in January 2018 gave staff a chance to feedback in further detail. The strategy was launched in April 2018.<br>Work has been underway to review the benefits offered to staff. An employee recognition group meets to consider options to improve the offer, including a new buying and selling of annual leave policy. | Annual survey and staff conferences – Yvonne Akinmodun/<br>Ongoing - 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). | In place – Paula Robinson |
| | Learning from Agile methodology to ensure we always have a clear 'definition of done' in place, and that we record when products/outputs have met the 'done' criteria and are deemed complete.<br>Agile approach to be brought into project processes under new project governance framework. | Partially in place – further work to be done by early 2018/19 - Paula Robinson |
| | Team-level service delivery planning for the next business year, with active involvement of team members. CMG will continue to review planning and delivery.<br>Requirement for this to be in place for each business year. | In place – Paula Robinson |
| | Planning and prioritising data submission project delivery, and therefore strategy delivery, within our limited resources. | In place until project ends in Autumn 2018 – Dan Howard |
| Possible future increase in capacity and capability needed to process and assess licensing activity including mitochondrial donation applications.<br>As at May 2018, the initial mitochondrial donation applications have taken up a significant amount of resource at | Licensing processes for mitochondrial donation are in place (decision trees etc).<br>An external review of the HFEA licensing processes has been carried out to assess current capabilities and processes and make changes for the future. This will be considered and where relevant implemented May – July 2018.<br>To mitigate the present capacity and capability issues, the executive has signed up more | Issue for further consideration – Clare Ettinghausen |

| | | |
|---|---|---|
| Statutory Approvals committee and for the executive in preparing papers and minutes. There have also been some issues with finding suitably experienced peer reviewers. | experienced mitochondria peer reviewers and have received feedback on the process and are in the process of making some administrative changes to address any capability concerns.<br>As at May, improvements to the application form have been agreed and these should ensure all of the right information is elicited, to prevent additional administration and/or unnecessary adjournments. | |
| Loss of knowledge in the Policy team given high-turnover of key individuals, including the Head during Q3/4 2017/18.<br>This will have a knock-on impact on other teams primarily Legal. | As above, knowledge transfer has been prioritised.<br>The team has been at complement since February 2018 and new starters have been thoroughly inducted, although it takes some time for new staff to get up to speed.<br>Policy work has been reprioritised with a focus on the Code of Practice October 2018 revision and key SMT/CE have been involved as and when needed. | In place - Clare Ettinghausen |
| Bedding down the new organisational structure to maximise organisational capability will necessarily involve some team building time, developing new processes, staff away days to discuss new ways of working, etc. This will be challenging given small organisational capacity and ongoing delivery of business as usual. | Continuing programme of leadership development for Heads and SMT.<br>Organisational development activity has continued, including summer awayday (10 July 2017), to support new ways of working development. A leadership awayday (November 2017) and another all staff awayday in January 2018 with a focus on building an HFEA culture following the organisational changes | Leadership development programme underway in Q1 and Q2 2018/19<br>Ongoing – Yvonne Akinmodun |
| Following organisational change implementation, 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.<br>Knowledge management via records management and documentation and Yvonne Akinmodun is reviewing onboarding methods as part of ongoing HR work. | In progress, – Peter Thompson<br>Underway Q1 2018/19 – Yvonne Akinmodun |
| The new organisational model may not achieve the desired benefits for organisational capability | The model will be kept under review following implementation to ensure it yields the intended benefits. | A review of the new model will be presented to AGC in June 2018 – Peter Thompson |
| Failure to appoint new Authority members before existing members' terms of office expire, leads to loss of knowledge and impacts on formal decision making. | As at May 2018, DHSC were considering four new Authority appointments. Chair/CEO in close contact with DHSC to press for an early decision. | Ongoing – Peter Thompson |
| **Risk interdependencies** | **Control arrangements** | **Owner** |

| | | |
|---|---|---|
| **(ALBs / DHSC)** | | |
| **Government/DHSC:**<br>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.<br>We have also been reviewed extensively (including the McCracken review and Triennial Review). | In place – Peter Thompson |

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

| **Inherent risk level:** | | | **Residual risk level:** | | |
|---|---|---|---|---|---|
| Likelihood | Impact | Inherent risk | **Likelihood** | **Impact** | **Residual risk** |
| 5 | 4 | 20 – Very high | **3** | **3** | **9 - Medium** |
| **Tolerance threshold:** | | | | | **6 - Medium** |

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

| Commentary |
|---|
| **Above tolerance.**<br>As at May 2018 the review of all IT policies is ongoing, to ensure that these remain fit for purpose. All new development has been done with cyber security in mind and this is especially true of the Register migration which will not be completed until we receive adequate external assurance of data security. This external assurance has been ongoing throughout the migration planning process. Penetration testing of the submission system was completed in April and May and this has provided us with further assurance that the system can withstand a cyber security attack.<br>In recent months the national cyber security risk has heightened and this is something the Chief Information Officer, his team and the SIRO have been acutely aware of. On reflection, in May we have revised the residual assessment of the impact of this risk, which reflects the real level of impact of such an attack were it to occur. Staff have been updated on the developing situation and we have responded to DHSC requests for assurance on cyber attacks to reassure them that our systems are fit for purpose. Following an automated attack on the patient rating feature on CaFC in February 2018, we added additional cyber security measures. |

| 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.<br>Internal audit report on data loss (October 2017) gave a 'moderate' rating, and recommendations are being actioned and reported to SMT on a monthly basis and at each AGC meeting.<br>A business continuity plan is in place. | Ongoing regular reporting - Nick Jones/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. | Penetration testing underway in April-May 2018 - Nick Jones/Dan Howard |
| There is a risk that IT demand could outstrip supply and so IT support doesn't meet the business requirements of the organisation and so we cannot identify or resolve problems in a timely fashion. | We continually refine the IT support functional model in line with industry standards (ie, ITIL).<br><br>We are actively improving our controls by investigating additional support delivered by a third party. This includes partnering with similar organisations such as the HTA, or entering into a separate agreement with an infrastructure support provider (it is likely that desktop support would remain unaffected by such an arrangement). | Approved per the ongoing business plan and budget agreement process – Dan Howard<br><br>Short term arrangement should be finalised in May. A longer-term support arrangement will be in place c. Autumn 2018 – 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.<br><br>All staff have annual compulsory security training to guard against breaches of confidentiality.<br><br>Relevant and current policies to support staff in ensuring high standards of information security.<br><br>There are secure working arrangements for the Register team and other relevant staff both in the office and when working at home (end to end data encryption via the internet, hardware encryption)<br><br>Further to these mitigations, any malicious actions would be a criminal act. | In place – Peter Thompson<br><br>As at May 2018, we are continuing to review and update key existing policies. To be completed by end Q1 2018/19 – Dan Howard |
| There is a risk that technical or system weaknesses lead to loss of, or inability to access, sensitive data, including the Register. | Back-ups of the data held in the warehouse in place to minimise the risk of data loss. Regular monitoring takes place to ensure our data backup regime and controls are effective.<br><br>We are ensuring that a thorough investigation takes place prior, during, and after migrating the Register. 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<br><br>Results of penetration testing in May were positive. The new Register will be in use from |

| | | |
|---|---|---|
| | | Autumn 2018 – Dan Howard |
| Business continuity issue (whether caused by cyber-attack, internal malicious damage to infrastructure or an event affecting access to Spring Gardens). | Business continuity plan and staff site in place. Improved testing of the BCP information cascade to all staff was undertaken in September 2017 as well as a tabletop test and testing with Authority members.<br>Existing controls are through secure off-site back-ups via third party supplier.<br>A backup environment has been set up to provide a further secure point of recovery for data which would be held by the organisation. As at May, the results of testing have been positive. | BCP in place, regularly tested and reviewed annually – Nick Jones<br>Undertaken monthly – Dan Howard<br>The new Register backup environment will come into use in the Autumn - Dan Howard |
| The corporate records management system (TRIM) is unsupported and unstable and we are carrying an increased risk of it failing. Alongside this, there is the risk of poor records management by staff.<br>The organisation may be at risk of poor records management until the new system is functioning and records successfully transferred. | A comprehensive review of our records management practices and document management system (TRIM) has started including the formation of a working group. A formal project will be initiated in July 2018 once initial scoping has been completed. | Project to be delivered within 2018/19 business year – Peter Thompson |
| Cloud-related risks. | Detailed controls set out in 2017 internal audit report on this area.<br>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.<br>Cyber-security is an 'in-common' risk across the Department and its ALBs. | | |

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

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

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

| Commentary |
|---|
| **At tolerance.**<br>As at May 2018, planning continues for the CaFC appeal hearing in October. The Chief Executive continues to engage with the appellant with a view to settling the case, but it is not yet possible to say whether a settlement is achievable.<br>There has been an increase in the number of storage consent cases coming to the HFEA from clinics that have failed to comply with the applicable statutory provisions on extension of storage. Whilst the facts and circumstances of some cases mean that it is possible to find a way forward, it is possible that one of these cases will end up in court which would cause significant resource diversion. We have therefore added this risk source below. |

| Causes / sources | Mitigations | Timescale / owner |
|---|---|---|
| Assisted reproduction is complex and controversial and the Act and regulations are open to 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.<br>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.<br>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<br>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 |
| Committee decisions or our decision-making processes may be contested. ie, Licensing appeals and/or JRs.<br><br>**Note**: Inspection rating on CaFC may mean that more clinics make representations against licensing decisions. | Panel of legal advisors in place to advise committees on questions of law and to help achieve consistency of decision making processes.<br><br>From Spring 2018 the Head of Legal has been working with the panel to ensure consistency of advice between the legal advisors from different firms. These include:<br>• Provision of previous committee papers and minutes to the advisor for the following meeting<br>• Annual workshop<br>• SharePoint site for sharing questions, information and experiences | In place – Peter Thompson<br><br>Ongoing – including the annual workshop with advisors – Catherine Drennan |
| | Maintaining, keeping up to date and publishing licensing SOPs, committee decision trees etc. to ensure we take decisions well.<br><br>Consistent decision making at licence committees supported by effective tools for committees.<br><br>Standard licensing pack distributed to members/advisers (refreshed in April 2018).<br><br>As at May 2018 the executive have been reviewing the findings of the final report of the licensing review to assess which changes will be implemented and how, to make the licensing process more efficient and robust. | In place, licensing SOPs have been refreshed in Q4 2017/18 and this will be further informed by the licensing review, to be discussed and implemented May-July 2018 – Paula Robinson |
| | Well-evidenced recommendations in inspection reports mean that licensing decisions are adequately supported and defensible. | In place – Sharon Fensome-Rimmer |
| Involvement of the Head of Legal in an increased number of complex Compliance management reviews and related advice impacts other legal work. | 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.<br><br>The Compliance management team will 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, Nick Jones |
| Moving to a bolder strategic stance, eg, on add ons or value for money, could result in claims that we are adversely | Risks considered whenever a new approach or policy is being developed. | In place – Clare Ettinghausen |

| | | |
|---|---|---|
| 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. | Business impact target assessments carried out whenever a regulatory change is likely to have a significant cost consequence for clinics.<br>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.<br>Major changes are consulted on widely. | |
| 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 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 CMG) in place to reprioritise workload should this become necessary. | In place – Peter Thompson |
| Adverse judgments require us to alter or intensify our processes, sometimes more than once. | Licensing SOPs being improved and updated, committee decision trees in place. | In progress (to complete in Q1 of 2018/19) and in place – Paula Robinson |
| HFEA process failings could create or contribute to legal challenges, or weaken cases that are otherwise sound, | Licensing SOPs being improved and updated, committee decision trees in place.<br>Advice sought through the Licensing review on specific legal points, so that improvements can be identified and implemented. | In progress (to complete in Q1 of 2018/19) and in place – Paula Robinson<br>To be discussed and implemented May-July 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 review now due Q1 2018/19 – Nick Jones / Sharon Fensome-Rimmer |

| | | |
|---|---|---|
| Storage consent failings at clinics are leading to a significant diversion of legal resource and additional costs for external legal advice. | We will be taking advice from a leading barrister on the possible options for a standard approach for similar cases.<br><br>The Head of Legal made significant amendments to guidance in the Code of Practice dealing with consent to storage and extension of storage. This guidance should mean that clinics are clearer about their statutory responsibilities. | In Q1 2018/19 – Catherine Drennan<br><br>Revised version of the Code comes into force October 2018 – 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. | GDPR work has been handled proactively, with a joint HFEA and HTA project team.<br><br>The GDPR project has been sponsored directly by the Director of Finance and Resources to ensure senior oversight.<br><br>AGC have regular updates on progress. | Project ongoing until October 2018 - Richard Sydee |
| **Risk interdependencies (ALBs / DHSC)** | **Control arrangements** | **Owner** |
| **DHSC:** HFEA could face unexpected high legal costs or damages which it could not fund. | If this risk was to become an issue then discussion with the Department of Health and Social Care would need to take place regarding possible cover for any extraordinary costs, since it is not possible for the HFEA to insure itself against such an eventuality, and not reasonable for the HFEA's small budget to include a large legal contingency. This is therefore an accepted, rather than mitigated risk. It is also an interdependent risk because DHSC would be involved in resolving it. | In place – Peter Thompson |
| **DHSC:** Legislative interdependency. | Our regular communications channels with the Department would ensure we were aware of any planned change at the earliest stage. Joint working arrangements would then be put in place as needed, depending on the scale of the change. If necessary, this would include agreeing any associated implementation budget.<br><br>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.<br><br>Sign-off for key documents such as the Code of Practice in place. | In place – Peter Thompson |

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

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

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

| **Commentary** |
|---|
| **At tolerance.**<br>Data submission work continues at a good pace. The background development work is on course to be completed in Spring 2018 and clinics will be using the new system by Autumn. However, completion is dependent on departmental capital cover, noted in detail below.<br>The work of the Intelligence team is well underway and the latest edition of Fertility Trends successfully launched in March 2018. The team's work focuses on improving the use of our existing data and making the most of the new Register post-migration. |

| **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. | The data submission project is well planned and under way after initial delays. Data Submission development work is now largely complete, with clinic implementation and access to it following by Autumn 2018.<br>Oversight and prioritisation of any remaining development work will be through the IT development programme board. | Completion of data submission project Autumn 2018 – Nick Jones |
| Risks associated with data migration to new structure, compromises record accuracy and data integrity. | Migration of the Register is highly complex. IfQ programme groundwork focused on current state of Register. There is substantial high-level oversight including an agreed migration strategy which is being followed. The migration will not go ahead until agreed data quality thresholds are met. | Autumn 2018 with regular reporting on progress prior to this – Nick Jones/Dan Howard |

| | | |
|---|---|---|
| | Work on the migration is broadly going to plan as at May 2018. | |
| 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.<br>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.<br>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 – Nick Jones |
| 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 will provide greater resilience against unforeseen issues or incidents. The IT systems manager is actively investigating a medium-term solution with an outsourced IT services provider. | In place with work underway to improve arrangements in Spring 2018 – 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. Business support and the inspection teams are at full complement.<br>Although not all systems are in place in relation to providing data to inspectors eg, patient feedback, workarounds are in place which are being monitored for their effectiveness. | In place – Nick Jones |
| Failure to integrate the new data and intelligence systems into Compliance activities due to cultural silos. | Work is underway in 2018 to further define and bed in HFEA culture in the light of organisational changes. The people strategy was launched in April 2018. | Ongoing, Q1 and 2 2018/19 - Yvonne Akinmodun |
| Regulatory monitoring may be disrupted if Electronic Patient Record System (EPRS) providers are not able to submit data to the new register structure until their software has been updated. | Earlier agreements to extend part of 'IfQ' delivery help to address this risk by extending the release date for the data submission project.<br>The Compliance management team are considering how to manage any centres with EPRS systems who are not ready to provide Register data in the required timeframe. This may include regulatory sanctions. Early engagement with EPRS providers means the risk of non-compliance is slim. | Plan in place to deal with any inability to supply data - Nick Jones |

| | | |
|---|---|---|
| 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 – Nick Jones |
| | We undertake an audit programme to check information provision and accuracy. | In place – Nick Jones |
| Excessive demand on systems and over-reliance on a few key expert individuals – request overload – leading to errors | PQs, FOIs and OTRs have dedicated expert staff/teams to deal with them although they are very reliant on a small number of individuals.<br>We have systems for checking consistency of answers. | In place – Clare Ettinghausen / Caylin Joski-Jethi |
| Risk that we do not get enough patient feedback to be useful / usable as soft intelligence for use in regulatory and other processes, or to give feedback of value to clinics. | During the patient feedback trial a communications strategy was in place, including considering ways to encourage more patient feedback.<br>The intelligence strategy focuses in part on making best use of the information gleaned from patients, and converting our mix of soft and hard data into real outcomes and improvements. This includes a new patient survey to be piloted in 2018 to give us qualitative and quantitative data on patient's experience of fertility treatment in the UK. | Plan to be developed post March 2018 – Clare Ettinghausen /Caylin Joski-Jethi/Jo Triggs |
| Failure to obtain capital cover for the remaining IfQ work would result in an inability to complete the programme and so realise the anticipated benefits.<br>Inadequate capital cover could also impact on some planned improvements to HFEA core IT systems (such as the document management system) with the result that there is an increased likelihood of failure for older systems. | Actively talking to DHSC and awaiting a response from minsters.<br>Reviewing the scheduling of the work to reduce the exposure to this issue.<br>Looking at alternative models to fund the changes, ie, making use of third party suppliers where appropriate.<br>A third party contract is in place to increase the resilience of the existing systems in the interim. | Ongoing - Nick Jones<br>Ongoing - Nick Jones<br>Ongoing - Nick Jones<br>In place - Nick Jones |
| Failure to obtain capital cover, resulting in non-completion of IfQ could lead to significant reputational costs as the promised benefits for clinics would not be delivered. | See above. | |
| **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.

| 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**<br>ME1: Messaging, engagement and information provision | Clare Ettinghausen<br>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<br>Safe, ethical effective treatment: Engender high quality research and responsible innovation in clinics.<br>Consistent outcomes and support: Increase consistency in treatment standards, outcomes, value for money and support for donors and patients. | ⇔⇔⇔⇔ |

| Commentary |
|---|
| **At tolerance.**<br>As at May, the status of this risk is generally positive. In March 2018 we released the latest edition of Fertility Trends which has made birth data from 2016 available to patients and the wider public and stakeholders. The report has been followed up on social media in the six weeks since release to boost its impact. The website was reviewed to ensure that all statistics were current.<br>Work is underway on a new publication and engagement strategy which will ensure that we publish information regularly and align this to other wider events.<br>A review of FOI processes and training will occur in 2018 to ensure that any further mitigations are identified and we strengthen our expertise. We do not therefore believe that this risk has risen at this point in time. |
| |

| 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. | Communications strategy in place, including social media and other channels as well as making full use of our new website. Stakeholder meetings with the sector in place to help us to underline key campaign messages.<br>The Communications team cannot do this in isolation and a good deal of communication with clinics occurs through the inspectorate. When there are messages that need to be conveyed to | In place – Jo Triggs<br>In place - Sharon Fensome-Rimmer, |

| | | |
|---|---|---|
| | clinics through the inspection team, Policy or Communications work with the team so that a co-ordinated approach is achieved. Equally, the inspection team keep abreast of all communications with the sector through Clinic Focus, Chairs letters etc.<br><br>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. | Laura Riley, and Jo Triggs |
| Patients and other stakeholders do not receive the correct guidance or information. | Policy team ensures guidance is created with appropriate stakeholder engagement and is developed and implemented carefully to ensure it is correct.<br><br>Ongoing user testing and feedback about the information on the website allows us to properly understand user needs.<br><br>We have internal processes in place which meet the Information Standard.<br><br>We are actively reviewing options for delivery of the Donor Conceived Register (DCR) to ensure the new service meets the needs of pre-1991 donor conceived people and is an improvement on the existing service. We are in regular communication with the chair of the DCR panel. We have agreed a four-month rolling contract with The National Gamete Donation Trust (current service providers) until a decision is made on the new service to ensure a smooth transition. We will regularly measure the quality of service and effectiveness after go-live. | In place – Laura Riley, Jo Triggs<br><br>In place –Jo Triggs<br><br>In place –Jo Triggs<br><br>Interim arrangement in place and ongoing plans being considered Q1 2018/19 - Nick Jones |
| We are not able to reach the right people with the right message at the right time. | We have an ongoing partnership with NHS Choices to get information to patients early in their fertility journey.<br><br>Planning for campaigns and projects includes consideration of communications channels.<br><br>When developing policies, we ensure that we have strong communication plans in place to reach the appropriate stakeholders.<br><br>Extended use of social media to get to the right audiences.<br><br>The communications team analyse the effectiveness of our communications channels in order to ensure that they continue to meet our user needs.<br><br>The new intelligence strategy has enabled the communications team to develop a further engagement strategy based around the reports that the intelligence team will be producing in 2018/19. | In place and developing – Jo Triggs<br><br>In place and ongoing – Jo Triggs<br><br>In place - Laura Riley, Jo Triggs<br><br>In place– Jo Triggs<br><br>Ongoing through Digital Communications Board meetings – Jo Triggs |

| | | |
|---|---|---|
| Risk that incorrect information is provided in PQs or FOIs and this may lead to misinformation and misunderstanding by patients, journalists and others.<br><br>As at May 2018, a number of people who are involved in FOIs are not trained in FOI practices and procedures, which means this risk is increased. | PQs, FOIs and OTRs have dedicated expert staff/teams to deal with them. However, as at May 2018, formal organisational training is required in relation to FOIs.<br><br>We have systems for checking consistency of answers and a member of SMT must sign off every PQ response before submission.<br><br>A future review of the FOI processes and procedures in the organisations This will include a review of general staff understanding of FOIs. | Training to be planned for later in 2018 - Clare Ettinghausen<br><br>Clare Ettinghausen /SMT - In place<br><br>Clare Ettinghausen – being planned, to occur Spring/Summer 2018 |
| 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 data on our website. | The Communications team ensure that public information reflects the latest knowledge from Intelligence and Policy. Intelligence and Policy teams take all steps to ensure that accurate information is provided to Communications.<br><br>The Communications team work quickly to amend any factual inaccuracies identified.<br><br>The Communications publication schedule includes a review of the website, to update relevant statistics when more current information is available. | In place - Caylin Joski-Jethi, Laura Riley, and Jo Triggs<br><br>In place – Jo Triggs<br><br>In place – Jo Triggs |
| **Risk interdependencies (ALBs / DHSC)** | **Control arrangements** | **Owner** |
| NHS Choices site and our site contain links to one another. | We maintain a relationship with the NHS Choices team. | |

## Reviews and revision

### SMT review – May 2018 (29/05/2018)

SMT made the following detailed points when reviewing the risk register:

- SMT discussed how the capital cover risk was reflected in the risk register. SMT considered that this was a risk to the delivery of regulatory improvements, rather than specific financial risk (albeit it related to organisational finances) and included the actions that were being undertaken to address this under the RE1 risk.
- When considering the C1 capability risk SMT noted the improvement in this area over the previous months; recent successful recruitments (developer and data analyst roles) had further improved the picture.
- SMT reflected on the scores of the Cyber Security risk and considered that the residual risk did not adequately reflect the real residual impact of any cyber breach which they felt was in fact higher given the general increase in hostile attacks. They increased the residual impact from 2 to 3, bringing the overall risk level up from 6 to 9. SMT were however reassured that all reasonable actions had been taken to control this risk, despite this now being above tolerance.
- Under the ME1 risk, SMT included commentary about a new risk mitigation, related to work being undertaken to ensure delivery of an effective new Donor Conceived Register.

### Authority review – May 2018 meeting (09/05/2018)

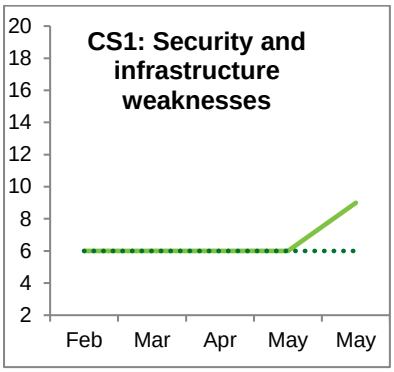
- Authority received the risk register and discussed the risks presented.
- Members discussed the risk to obtain capital cover for remaining IfQ work (and other IT enhancements). Members heard that this was not an area where there were finance mitigations per-se, other than the Director of Finance and Resources staying in close contact with DHSC and making the case to have capital cover granted. Members stressed the need to properly reflect the risks and mitigations around a potential failure to obtain capital cover, these may be business rather than financial risks and mitigations.
- Members raised an upcoming risk around the loss of member knowledge as Authority and SAC member terms finished, this would be an additional source of capability risk.
- Members discussed the cyber risk and the Authority's responsibilities for holding personal data securely. Members heard that this was of the highest priority to the executive and every care was taken to assure the security of the register. Members noted that it was very important that members were kept up to date about cyber security as otherwise they could inadvertently expose the organisation to risk.
- A member noted the importance of acknowledging it is not desirable to reduce every risk – the aim should not be to artificially reduce all risks to green – sometimes a higher level of risk may be accepted for a time and this was appropriate.

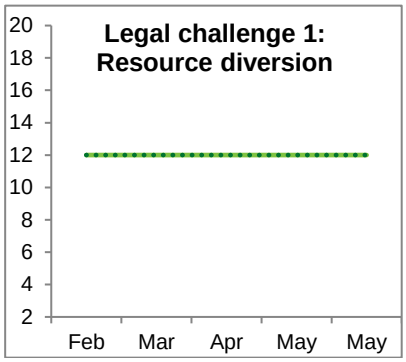
### SMT review – April 2018 meeting (16/04/2018)

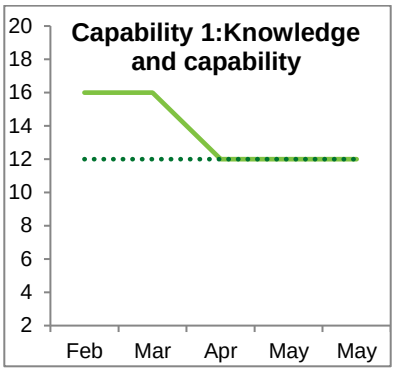
- SMT considered the finance risk and agreed that by the time of the Authority meeting it would be clearer what risk remained in relation to finances and whether the risk score should be changed.
- SMT agreed to remove the organisational change risk as agreed with the Authority. Elements of the risk were moved to other risk sources as appropriate.
- SMT agreed that it now felt appropriate to reduce the score of the capability risk to at tolerance. Particular capability issues, such as that created by turnover in policy team were being addressed and though the developer role had proved more difficult to recruit for, temporary developer resource was in place to cover some of this capability gap. SMT agreed that the improvements that were underway to increase the learning, development and recognition offer would help boost organisational capability and address the risk of further loss of staff...

# Tolerance vs Residual Risk:

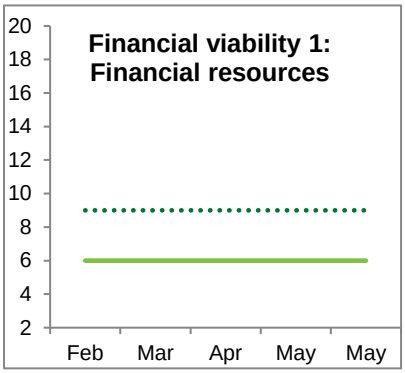
## High and above tolerance risks

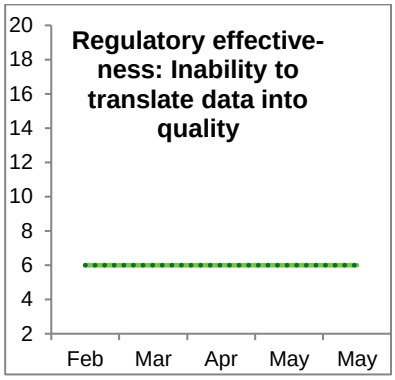


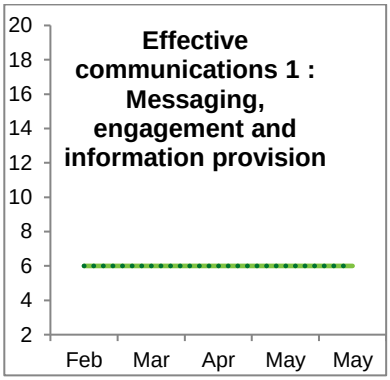




## Lower level / in tolerance risks



## 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 |
| Risk Score = Impact x Likelihood | Likelihood | | | | |

## Risk appetite and tolerance

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

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

## Assessing inherent risk

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

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

## System-wide risk interdependencies

As of April 2017, we explicitly consider whether any HFEA strategic risks or controls have a potential impact for, or interdependency with, the Department or any other ALBs. A distinct section to record any such interdependencies beneath each risk has been added to the risk register, so as to be sure we identify and manage risk 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 | 12 | | |
| Paper number | AGC (12/06/2018) 613 | | |
| Meeting date | 12 June 2018 | | |
| Author | Morounke Akingbola, Head of Finance | | |
| **Output:** | | | |
| For information or decision? | Decision | | |
| Recommendation | The Committee is asked to review and make any further suggestions and comments and agree the plan. | | |
| Resource implications | None | | |
| Implementation date | N/A | | |
| Organisational risk | ☒ Low | ☐ Medium | ☐ High |
| | Not to have a plan risks incomplete assurance, inadequate coverage or unavailability key officers or information | | |
| Annexes | N/A | | |

# Audit & Governance Committee Forward Plan

| AGC Items Date: | 6 Mar 2018 | 12 Jun 2018 | 9 Oct 2018 | 4 Dec 2018 |
|---|---|---|---|---|
| Following Authority Date: | 9 May 2018 | 27 Jun 2018 | 14 Nov 2018 | Jan 2019 |
| **Meeting 'Theme/s'** | **Finance and Resources** | **Annual Reports, Information Governance, People** | **Strategy & Corporate Affairs, AGC review** | **Register and Compliance, Business Continuity** |
| **Reporting Officers** | **Director of Finance & Resources** | **Director of Finance & Resources** | **Director of Strategy & Corporate Affairs** | **Director of Compliance and Information** |
| Strategic Risk Register | Yes | Yes | Yes | Yes |
| Information for Quality (IfQ) Prog | Yes | Yes | Yes | Yes |
| Annual Report & Accounts (inc Annual Governance Statement) | | Yes – For approval | | |
| External audit (NAO) strategy & work | Interim Feedback | Audit Completion Report | Audit Planning Report | Audit Planning Report |
| Information Assurance & Security | | Yes | | |
| Internal Audit Recommendations Follow-up | Yes | Yes | Yes | Yes |
| Internal Audit | Update | Results, annual opinion approve draft plan | Update | Update |
| Whistle Blowing, fraud (report of any incidents) | Update as necessary | Update as necessary | Update as necessary | Update as necessary |
| Contracts & Procurement including SLA management | Update as necessary | Update as necessary | Update as necessary | Update as necessary |

| AGC Items Date: | 6 Mar 2018 | 12 Jun 2018 | 9 Oct 2018 | 4 Dec 2018 |
|---|---|---|---|---|
| HR, People Planning & Processes | | Yes Including bi-annual HR report | | Yes - Bi-annual HR report |
| Strategy & Corporate Affairs management | | | Yes | |
| Regulatory & Register management | | | | Yes |
| Resilience & Business Continuity Management | Yes | Yes | Yes | Yes |
| Finance and Resources management | Yes | | | |
| Reserves policy | | | Yes | |
| Estates | | June | Yes | Yes |
| Review of AGC activities & effectiveness, terms of reference | Yes | | | Yes |
| Legal Risks | | | Yes | |
| AGC Forward Plan | Yes | Yes | Yes | Yes |
| Session for Members and auditors | Yes | Yes | Yes | Yes |
| Other one-off items | | | HFEA Risk Policy | |