# Audit and Governance Committee meeting - agenda

Human Fertilisation & Embryology Authority

## 13 June 2017

## Abbey Room

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

| Agenda item | | | Time |
|---|---|---|---|
| 1. | Welcome, apologies and declaration of interests | | 10:00am |
| 2. | Minutes of 21 March 2017<br>**[AGC (13/06/2017) 541]** | For Decision | 10.05am |
| 3. | Matters Arising<br>**[AGC (13/06/2017) 542 MA]** | For Information | 10.10am |
| 4. | Internal Audit<br>a) Annual Assurance Statement 2016-17<br>**[AGC (13/06/2017) 543 DH]**<br>b) 2017/18 Plan<br>**[AGC (13/06/2017) 544 DH]** | <br>For Decision<br><br>For Information | 10.15am |
| 5. | Implementation of Audit Recommendations<br>**[AGC (13/06/2017) 545 RS]** | For information | 10.30am |
| 6. | Annual Report and Accounts<br>**[AGC (13/06/2017) 546 RS]** | For Decision | 10.35am |
| 7. | External Audit – Audit Completion Report<br>**[AGC 13/06/2017) 547 NAO]** | To follow | 11.05am |
| 8. | HR – Update on reorganisation and post staff survey<br>**[AGC (21/17/2017) 548 PT]** | Verbal Update | 11.25am |
| 9. | Information for Quality (IfQ) Programme<br>**[AGC (13/06/2017) 549 NJ]** | For Information | 11.35am |
| 10. | Information Assurance and Security<br>**[AGC (13/96/2017) 550 DM]** | Verbal Update | 11.45am |
| 11. | Cyber Security<br>**[AGC (13/06/2017) 551 DM]** | For Information | 11.50am |
| 12. | Resilience & Business Continuity Management<br>**[AGC (13/06/2017) 552 DM]** | For Information | 11.55am |
| 13. | ALB Risk Interdependencies | For Discussion | 12.05pm |

| | | | |
|---|---|---|---|
| | **[AGC (13/06/2017) 553 PR]** | | |
| 14. | Strategic Risks 2017/18<br>**[AGC (13/06/2017) 554 PR]** | For Discussion | 12.15pm |
| 15. | AGC Forward Plan<br>**[AGC (13/06/2017) 555 MA]** | For Decision | 12.30pm |
| 16. | Whistle Blowing and Fraud<br>**[AGC (13/06/2017) 556 RS]** | Verbal update | 12.35pm |
| 17. | Contracts and Procurement<br>**[AGC (13/06/2017) 557 MA]** | Verbal update | 12.45pm |
| 18. | Any other business | | 12.55pm |
| 19. | Close (Refreshments & Lunch provided) | | 1.00pm |
| 20. | Session for members and auditors only | | 1.00pm |
| 21. | Next Meeting 10am Tuesday, 3 October 2017, 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 (13/06/2017) 541 | | |
| Meeting date | 13 June 2017 | | |
| Author | Bernice Ash, Committee Secretary | | |
| **Output:** | | | |
| For information or decision? | For decision | | |
| Recommendation | Members are asked to confirm the minutes as a true and accurate record of the meeting | | |
| Resource implications | | | |
| Implementation date | | | |
| Communication(s) | | | |
| Organisational risk | ☐ Low | ☐ Medium | ☐ High |
| Annexes | | | |

## Minutes of Audit and Governance Committee meeting held on 21 March 2017

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

| | |
|---|---|
| Members present | Anita Bharucha (Chair)<br>Margaret Gilmore<br>Gill Laver<br>Jerry Page |
| Apologies | None |
| External advisers | Internal Audit - PricewaterhouseCoopers (PwC):<br>Paul Foreman<br><br>External Audit - National Audit Office (NAO):<br>Sarah Edwards<br>George Smiles |
| Observers | Jeremy Nolan, Head of Internal Audit, DH (from 1 April 2017)<br>Kim Hayes, Department of Health |
| Staff in attendance | Peter Thompson, Chief Executive<br>Morounke Akingbola, Head of Finance<br>Richard Sydee, Director of Finance & Resources<br>Nick Jones, Director of Compliance and Information<br>Paula Robinson, Head of Business Planning<br>Erin Barton, Governance Manager<br>Bernice Ash, Committee Secretary |

# 1. Welcome, apologies and declarations of interests

**1.1** The Chair welcomed attendees to the meeting, in particular:

- Jeremy Nolan, taking up his DH appointment as Head of Internal Audit on 1 April 2017, attending his first Audit and Governance Committee meeting.
- Bernice Ash, Committee Secretary for the Audit and Governance Committee.

**1.2** Apologies had been received from Siobhain Kelly, Interim Head of Corporate Governance and David Moysen, Head of IT.

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

## 2. Minutes of the meeting held on 7 December 2016

**2.1** Subject to the amendment of point 8.3 to state that the 'field work on Cyber Security Terms of Reference was in the process of completion', the minutes of the meeting held on 7 December 2016 were agreed as a true record of the meeting and approved for signature by the Chair.

**2.2** The Chair requested the first draft of the minutes be circulated to all Committee members for comment. The minutes would then be finalised by the Chair and Committee Secretary for approval by the Committee at the next meeting.

## 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** 9.6) Report progress on actions from information governance group. This was an agenda item and therefore the committee agreed it could be removed from the matters arising.

**3.3** 12.6) Review of the procedures for representations. This item had been moved to Q3 2017/18 of the Business Plan and might be outsourced. The Committee agreed this item could be removed from the matters arising.

**3.4** 14.5) The HFEA had concluded work on the Triennial review report and the Committee agreed this item could be removed from the matters arising. The Chief Executive confirmed the draft report and action plan would be shared with Committee and Authority members.

**3.5** 5.7) Circulate a list of recommendations/actions (relating to public beta). The Committee agreed this this could be removed from the matters arising, noting it would have been beneficial for the list of recommendations and planned actions, to have been circulated in a timely manner.

**3.6** Items 11.6 and 13.5 relating to updates on cyber security and business continuity have been addressed in the items on the agenda below.

**3.7** 14.5) Head of HR to provide clarification on 6.4 in the Whistleblowing policy. Clarification was given that individuals raising concern are entitled to independent advice. The Committee agreed this item could be removed from the matters arising.

### Action

**3.7** The Chief Executive to circulate the draft Triennial review report and action plan to Committee and Authority members.

## 4. Internal Audit

### a) Introduction to HIA

**4.1** The new Head of Internal Audit for HFEA with effect from 1 April 2017 introduced himself to the Committee.

### b) Internal Audit Progress Report

**4.2** The Head of Internal Audit provided the Committee with a progress report on internal audits, particularly noting that additional time had been spent on the Cyber security threat.

**4.3** The Committee was informed that the plan was essentially complete and no high priority issues had been identified.

## c) Board Effectiveness – Final Report

**4.4** The Chair introduced the Final Report of the Review of Board Effectiveness noting there had been a high level of participation. The outcome of the review had shown that HFEA were above the benchmark in all aspects assessed. The review had also identified areas where improvements could continue to be made.

**4.5** The Head of Internal Audit noted this was a positive report. There were two recommendations for further action, one of which was rated medium relating to communication and the other low relating to training.

**4.6** It was identified that point 3.4 of the documentation incorrectly stated 'Lower than average results were received in the following categories'; it was agreed this sentence would be removed.

**4.7** The Committee observed that the distinctive role of Authority member meant they were involved in some operational issues, and that they felt closely engaged with the Authority's work as a result: this may have contributed in part to the Authority attaining scores well above the average benchmark.

**4.8** The Chief Executive stated that the Board was constituted of very good members who were committed to the HFEA; the Board was consistent and had a coherent sense of themselves.

**4.9** In discussion the Committee noted the significant workload for Authority members. The Committee discussed the importance of balancing the need to refresh membership of the board with maintaining continuity of expertise, while noting that appointments were a matter for Ministers.

**4.10** The Committee acknowledged that it was good practice for Board and Committee Chairs to identify any training needs of the members. It was noted that the Statutory Approvals Committee had received genetics training and a session had been held on mitochondrial transfer for relevant members.

**4.11** One member noted that she was no longer receiving the weekly media update, which was a useful document.

**4.12** The Chair concluded that the results of the Board effectiveness self-assessment placed the HFEA in a strong position going forward, particularly noting the positive leadership tone set by the Authority Chair and the effective working relationships between staff and Authority members.

### Actions

**4.13** The first sentence at point 3.4 of the report to be removed.

**4.14** The Chief Executive to ensure all Authority members receive the weekly media update.

## d) Information Standards – Final Report

**4.15** The Committee noted that the report focused on the published corporate information on the HFEA's new website, and the organisation's review of the information production process.

**4.16** The Committee was informed that nine cases had been identified, where no written evidence could be located that formal final approval had been given before draft publications had been released to the website. However, it had been confirmed that these had been given verbal approvals. A tightening up on this process is required and it was identified this is not currently listed on the Strategic Risk Register. The Chief Executive stated that procedures need to be more clearly evidenced and the organisation would improve in this area.

## e) Cloud Cyber Risk Assessment (advisory audit) and Cyber Security (Item 8)

**4.17** The Head of Internal Audit explained that the cloud cyber risk assessment was in draft stage, with the final version to be produced following the recently received management review and comments. The review had been commissioned to identify security risks relating to a cloud environment, to identify any risks to HFEA's security and to assess the controls in place. It was noted that, at the time of drafting the report, penetration testing had not commenced.

**4.18** Two recommendations had been made in the report relating to cloud lock-in and business continuity. With regards to cloud lock-in, it was recommended that HFEA update their Change Management Policies to reduce the likelihood of the organisation becoming totally reliant on Microsoft Azure in the future. The second recommendation related to business continuity if office connectivity to the cloud was ever lost.

**4.19** The Committee raised some concern with regards to IT security and the exposure to breaches when using the cloud. They were assured the risk remains the same as currently, whilst operating from a server. A restore and recover plan was in place should network failure occur.

**4.20** The Director of Compliance and Information spoke to the cyber security paper, stating that robust steps have been taken by the HFEA to ensure systems were being developed in a secure way and hosted securely. At the outset of the IfQ programme, an expert 'CLAS' consultant had been commissioned to provide policy guidance and assistance on the security of communications and electronic data. The Director of Compliance and Information stated that internal audit's approach regarding cloud cyber risk assessment had been very helpful.

**4.21** The Committee was informed that penetration testing had been performed against the Beta Portal site in January and February 2017. This had identified a number of vulnerabilities, which had been considered and addressed. The same 'live' assessment and penetration testing will be adopted for the launch of the HFEA website.

**4.22** The Committee asked if currently, any global information on cyber attacks is being collected as it would be useful to understand current activity of this nature. The Director of Compliance and Information confirmed this data is collected but would clarify how often and how this reporting was reviewed by Head of IT.

**4.23** The Committee also questioned whether training will be provided with regards to cyber security and how many people have access to central information held by the HFEA. The Committee was assured that a robust approach was taken regarding access to information according to access rights. Information security training is identified as a key component of a secure system and is in

place for all staff. It was noted the Head of IT is currently undertaking a week-long mandatory training course on cyber security provided by NHS Digital to all system Heads of IT.

## Action

**4.24** The Director of Compliance and Information to check how known cyber-attack threat data is collected and reviewed.

### f) Final Report and Annual Opinion

**4.25** The Committee was informed that the content of the final report would cover the areas previously discussed at the meeting, so should be rated as moderate. The IfQ work and Board effectiveness had been favourable and it was important this is drawn out in the annual governance report.

### g) Implementation of Recommendations

**4.26** The Head of Finance reported there had been seven new recommendations, with two noted as medium and five as low. The Board effectiveness recommendation is due for completion by 30 May 2017. The Head of Engagement had confirmed that the first recommendation on information standards work had been completed, with the remainder due by April 1. The cloud cyber risk assessment had one action due for completion by the end of April.

## 5. External Audit – Interim Feedback

**5.1** The NAO reported the interim audit at the HFEA had just been completed. There were no significant issues identified and everything was on track for the year end. The NAO would be visiting a clinic based in Cambridge in April as this is part of the audit process.

## 6. Finance and Resources Update

**6.1** The Director of Finance & Resources gave a presentation identifying the key risks in finance and resources.

**6.2** The key financial risks were noted as being concentration of knowledge in few finance staff, financial systems and interdependencies with IfQ release 2 and uncertain treatment fee income and expenditure relating to legal issues.

**6.3** The Director of Finance and Resources noted that due to staff changes within Finance, there is currently enormous corporate knowledge dependency on the Finance & Accounting Manager. The interdependency between the data submission portal and the system that underpins invoicing creates a potential risk around IfQ Release 2. It is crucial the testing around invoice information is thorough. It was noted that there is 6 months of operational income available as a reserve should issues arise.

**6.4** The Committee was informed of the difficulties in predicting annual legal expenditure. The Director of Finance & Resources reported that the forecast for the current financial year is £630,000 to year end. There still remain legal cases to be resolved before we reach the final year end position.

**6.5** The Director of Finance & Resources addressed the Committee regarding the emerging DH Estates plans which are set to be implemented in 2020/21. The current lease at 10 Spring

Gardens expires on the same timescale. This DH plans could result in offices being moved out of central London to areas in zones 2 and 3, to accommodation “hubs”.

**6.6** The Committee noted that Information Governance was being affected by IfQ and other priorities which is a risk to the HFEA. The new IT arrangements and future change of office could all affect business continuity, another potential risk which is being monitored.

**6.7** The Committee was provided with information regarding the current shared resources. The Head of Finance and the Director of Finance & Resources cover the HFEA and Human Tissue Authority (HTA), therefore needing to share resources, particularly to cover organisational priorities including attending Authority, Committee and Senior management meetings. This seems to be working.

**6.8** The Committee noted that year end processes create workload pressures but the Chief Executives at both the HFEA and HTA are pleased with the arrangements and balance of work for the Head of Finance and Director of Finance & Resources.

**6.9** The Chief Executive provided the Committee with an explanation of the organisational change currently occurring at the HFEA. The Committee was informed that the main drivers for change were the new strategy and IfQ which provide new possibilities for the organisation and the requirement for some different staff skill sets. A proposal had been circulated to staff in February and a formal proposal had now been issued, with affected staff being spoken to on an individual basis. The final proposal was scheduled to be presented to the Remuneration and Nominations Committee in late March.

**6.10** The Chair and Committee congratulated the Director of Finance & Resources on his achievements to date.

## 7. Information Governance Group Activities

**7.1** The Director of Finance & Resources reported that the Information Governance Group has not met. The organisational change proposals identifies an Information Governance Manager post, to provide the capacity to provide focus on this from now.

## 8. Resilience & Business Continuity Management

**8.1** The Director of Compliance and Information reported that business continuity has a dedicated site in Office 365, where an up to date copy of the Business Plan is stored and all staff can access this.

**8.2** The committee was informed that a test of the emergency alert system, that sends text to all staff members, was conducted on 1 March 2017. Only around 50% of staff responded to this text, with the reasons for this disappointing level of engagement being investigated. In any event reasons were likely to include some staff not updating the register of ‘phone numbers; difficulties logging in to the O365 site due to slightly different login credentials, and some apathy.

**8.3** The Committee noted this presents an element of risk. Concern was voiced over how Board and Committee members would receive these type of alerts. This Chief Executive confirmed this was a good point to raise and would require some thought.

**8.4** The Director of Compliance and Information referred to the last business continuity incident whereby power was lost at Spring Gardens for three days. A majority of staff were able to work at home as the move to Office 365 left email services unaffected.

**8.5** The Chief Executive stated the need to tighten up operationally on business continuity policies.

### Action

**8.6** The Director of Information and Compliance to review the reasons for the limited engagement to the 1 March 2017 emergency text alert, review plans and processes in the light of lessons learned and provide an update to the next Committee meeting.

## 9. AGC Forward Plan

**9.1** The Head of Finance reported that the Forward Plan, in its current form, had not changed since last year.

**9.2** The Chair suggested that IfQ remains as an item for all meetings going forward so the Committee remains engaged with developments and can scrutinise benefits realisation.

**9.3** The Committee agreed a draft version of the Annual Governance Statement should be circulated by email before the June meeting.

**9.4** The Committee agreed that Resilience and Business Continuity Management should remain an agenda item. The NAO confirmed that the audit planning report would be presented at the October meeting. A more substantial piece on cyber security should also be on the October meeting agenda.

### Action

**9.5** The Forward Plan to be amended to reflect the changes agreed by the Committee.
**9.6** Director of Resources to circulate the draft Annual Governance Statement during April.

## 10. Strategic Risk Register

**10.1** The Head of Business Planning presented the strategic risk register.

**10.2** The Committee was informed that Corporate Management Group (CMG) conducted its last review of the risk register for 2016/17 on 8 February 2017. At this meeting, it was agreed to merge the two risks relating to donor conception into a single risk relating to the quality of the Opening the Register Service, and to add a new risk on the forthcoming planned organisational changes. Four of the twelve risks are currently above tolerance.

**10.3** A new version of the strategic risk register would be presented at the next meeting, reflecting the new strategy, perhaps with the addition of cyber security as a separate risk. The Committee was informed that system risk interdependencies (with other ALBs and DH) would also be included on the next strategic risk register.

**10.4** The Head of Business Planning particularly highlighted the risks pertaining to IfQ, with reference to the delay of release 2. The Committee was also informed of the ongoing risk with regards to PQs, partly as a result of the loss of an expert staff member in the policy team, but also the volume, unpredictability and complexity of the PQs the HFEA receives.

**10.5** The Head of Business Planning informed the Committee of the risks concerning legal challenge.

**10.6** In relation to the risk on organisational change, the Chief Executive reiterated that all staff had been made aware of the forthcoming organisational change before Christmas 2016, that those directly involved had received individual letters of communication and that some formal interviews had occurred.

**10.7** The Committee was informed that members of the Authority had raised concern over issues such as redeployment opportunities and access to training for those individuals at risk, but had been reassured by the plans set out by the Chief Executive to address these.

**10.8** The relative timing of the Authority and Audit and Governance Committee meetings was also raised as a slight issue. It was noted that ideally, the strategic risk register should be presented to CMG, then the Committee, finally followed by the Authority. That would remain the aim, although occasional variations in this order may be unavoidable, depending on scheduling variables.

### Action

**10.9** Head of Business Planning to ensure when the next year's calendar of meetings was planned, that wherever possible AGC consideration precedes the Authority receiving the strategic risk register.

## 11. Information for Quality (IfQ) Programme

**11.1** The Director of Compliance and Information provided the Committee with an overview of the key issues.

**11.2** The Committee was informed that the clinic portal went live in January 2017 with only a few teething issues. It was hoped to launch the new HFEA website in April 2017. A GDS assessment had occurred, identifying a few areas requiring work, although none of significant concern. The launch of the website was currently prevented by the judicial review proceedings relating to the proposals for publishing performance measures within Choose a Fertility Clinic (CaFC). The outcome of the judicial review was still not known. It was noted that some residual work on the data submission portal was also still outstanding.

**11.3** The Director of Compliance and Information informed the Committee that, at the last Authority meeting (a few days before this meeting), it had agreed to the proposal formally to close the programme, at the appropriate time. The outstanding work would be taken forward as a separate project within the new business plan. The Authority noted that IfQ should continue to be discussed at Audit and Governance Committee meetings.

**11.4** The Committee was notified that contractual commitments with Reading Room, the principal supplier, had almost concluded.

**11.5** It was also noted that whilst work on the data submission component of the portal was ongoing and much had been achieved relating to data cleansing and other preparatory work for the future

Register migration, the new data submission product will not be ready for launch until the summer of 2017. Whilst the necessary resources to complete the project have been identified, discussions continue with the Department of Health relating to permission to 'cover' the additional capital expenditure necessary (approximately £300k). The Committee noted that this would represent a significant overspend on the overall IfQ budget.

**11.6** The Chief Executive noted the importance of continuing to keep the systems under iterative review afer the conclusion of the programme, to keep them up to date and responsive to user feedback.

**11.7** The Chair thanked all staff involved in IfQ for their work, recognising that this had been considerable.

## 12. Whistle Blowing and Fraud

**12.1** The Director of Finance & Resources informed the Committee there were no cases of whistle blowing or fraud to report.

## 13. Contracts and Procurement

**13.1** The Head of Finance reported that one contract had been let since the last meeting to Manchester University for Patient information (treatments) for the new Website.

## 14. Any other business

**14.1** This Chair, on behalf of the members and Executive, thanked the Head of Internal Audit for all his contributions to the Audit and Governance Committee.

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

**14.3** The next meeting will be held on Tuesday, 13 June 2017 at 10am.

## Chair's signature

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

**Signature**

**Name**

Anita Bharucha

**Date**

13 June 2017

# Audit and Governance Committee Paper

| | |
|---|---|
| **Paper Title:** | Matters arising from previous AGC meetings |
| **Paper Number:** | [AGC (13/06/2017) 542 MA] |
| **Meeting Date:** | 13 June 2017 |
| **Agenda Item:** | **3** |
| **Author:** | Morounke Akingbola, Head of Finance |
| **For information or decision?** | Information |
| **Recommendation to the Committee:** | To note and comment on the updates shown for each item. |
| **Evaluation** | To be updated and reviewed at each AGC. |

Numerically:

- 8 items added from March 2017 meeting,1 ongoing
- 2 items carried over from earlier meetings, 1 ongoing

| ACTION | RESPONSIBILITY | DUE DATE | PROGRESS TO DATE |
|---|---|---|---|
| **Matters Arising from Audit and Governance Committee – actions from 7 December 2016 meeting** | | | |
| **11.6** Head of IT to provide the Audit and Governance Committee with regular updates on Cyber Security. | Head of IT | | **Ongoing –** Agenda item for June 2017 meeting |
| **13.5** Head of IT to provide the Audit and Governance Committee with an update on resilience and business continuity at a future meeting, | Head of IT | March 2017 | **Completed** – Agenda item for June 2017 meeting |
| **Matters Arising from Audit and Governance Committee – actions from 21 March 2017 meeting** | | | |
| **3.7** The Chief Executive to circulate the draft Triennial review report and action plan to Committee and Authority members. | Chief Executive | June 2017 | **Completed** – Email sent to Members |
| **4.13** The first sentence at point 3.4 of the report to be removed | PwC | March 2017 | **Completed –** Amended on 22 March 2017 |
| **4.14** The Chief Executive to ensure all Authority members receive the weekly media update. | Chief Executive | N/a | **Completed** – Media Manager provides this |
| **4.24** The Director of Compliance and Information to check how known cyber-attack threat data is collected and reviewed. | Director of Compliance and Information | | **Completed** - Agenda item for June 2017 meeting |
| **8.6** The Director of Compliance and Information to review the reasons for the limited engagement to the 1 March 2017 emergency text alert, review plans and processes in the light of lessons learned | Director of Compliance and Information | June 2017 | **Completed** - Agenda item for June 2017 meeting |

| | | | |
|---|---|---|---|
| and provide an update to the next Committee meeting. | | | |
| **9.5** The Forward Plan to be amended to reflect the changes agreed by the Committee. | Head of Finance | June 2017 | **Completed -** Presented to Committee at June meeting |
| **9.6** Director of Resources to circulate the draft Annual Governance Statement during April. | Director of Resources | April 2017 | **Completed –** Circulated on 21 April 2017 |
| **10.9** Head of Business Planning to ensure when the next year's calendar of meetings was planned, that wherever possible AGC consideration precedes the Authority receiving the strategic risk register. | Head of Business Planning | September 2017 | **In progress -** Head of Planning & Governance will review when she looks at planning for 18/19 in August 2017. |

# ANNUAL ASSURANCE REPORT 2016/17

## *Human Fertilisation and Embryology Authority*

*DRAFT*

Health Group Internal Audit Service

## Background

In order to be able to provide an annual opinion for 2016/17 to the Human Fertilisation and Embryology Authority's (HFEA) Accounting Officer, it is necessary to consider the work undertaken by Internal Audit over the course of the 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 all sources of assurance (including the NAO) 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 2016/17 as well as including the formal annual opinion of the Head of Internal Audit.

## Executive Summary

Over the last few years, the Human Fertilisation and Embryology Authority has developed its regulatory model and executive and non-executive management have undertaken work to ensure that the organisation's governance structures including internal control and risk management arrangements remain fit for purpose. In 2016/17 there has in particular been focus on the development of HFEA's new website and clinic portal, a major project in which management has sought to manage the not insignificant risks associated with moving to a Cloud-based IT environment, developing and launching a new public-facing website and implementing a new portal through which centres will submit information to the Authority. The public website is currently in the beta testing phase.

Our recent report on management of the Cyber Security risk in relation to the move to the cloud environment, together with project gateway reviews and the results of third party penetration testing, has provided assurance to support the Audit and Governance Committee's close monitoring of the project. While the full implementation of the new website and systems has yet to be completed, at this stage it would appear that the Authority has shown itself to be risk-aware and to have taken reasonable steps to mitigate the key risks identified.

Our opinion is based solely on our assessment of whether the controls in place support the achievement of management's objectives as set out in our 2016/17 Internal Audit Plan and Individual Assignment Reports.

We used the following levels of rating (in line with the agreed definitions across all central 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. |

## 2016/17 Performance Summary

| | |
|---|---|
| **2016/17 agreed programme** | **5** |
| **Total reviews deferred to complete in 2017/18** | **0** |
| **Cancelled or Deferred reviews -** Assurance mapping agreed not to be undertaken, with resources re-deployed into a wider scope for the review of Cyber Penetration Threat Management | **(1)** |
| **Total reviews to be delivered per final 2016/17 programme** | **4** |
| | |
| **Total reviews completed in 2016/17** | **4** |
| **% of final programme completed** | **100%** |

## Total Number of Audits completed by rating

| Total no reviews completed 2016/17 | Substantial | Moderate | Limited | Unsatisfactory | Advisory | Total Rated Work | Advisory Work |
|---|---|---|---|---|---|---|---|
| 4 | 0 | 3 | 0 | 0 | 1 | **3** | **1** |
| | | | | | | **75%** | **25%** |

Our 2016/17 programme included one review which was an advisory review. This was a self-assessment of board effectiveness by the HFEA's board members, supported by internal audit interviewing members and mapping the findings against a benchmark based on other organisations for whom we had undertaken similar exercises. The self-assessment rated all areas within scope above the rating of the other comparator organisations. Whilst the nature of this work means that it was not appropriate to formally provide an assurance rating the outcome, the general observations and comments have been considered and taken into account where relevant in forming our overall opinion for the year.

## Resources 2016/17

| Period | Audit days | | | Comments |
|---|---|---|---|---|
| | **Budget** | **Actual** | **Variance** | |
| **April 2016 to March 2017** | **40** | **33** | **(7)** | A richer skill mix was required to deliver both Board Effectiveness and Cyber Threat reviews. Accordingly, fewer days of more senior staff have been used to deliver the programme. |

## Internal Audit Plan 2016/17 Delivery - Assurance and Advisory Work Summary

The reviews completed during the year are summarised below:

| # | Audit Title | Status | Outcome | Recommendations agreed by priority | | |
|---|---|---|---|---|---|---|
| | | | | High | Medium | Low |
| 1 | Income generation process/ Quality and efficiency of revenue data | Complete | Moderate | 0 | 1 | 4 |
| 2 | Information standards | Complete | Moderate | 0 | 1 | 2 |
| 3 | Board Effectiveness | Complete | Not rated | 0 | 0 | 2 |
| 4 | Management of Cyber Penetration threat | Complete | Moderate | 0 | 0 | 2 |
| | | | **Total** | **0** | **2** | **10** |

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

Health Group Internal Audit Services (HGIAS) was subject to an external quality assessment of its services in March 2016. The requirement of HM Treasury is that this should be undertaken at least every 5 years. At that time, HGIAS was rated as Generally Conforms.

Another external assessment was not required to be performed during 2016/17. However, HGIAS has continued to monitor and report on KPIs and quality assurance arrangements have continued to be applied to all outputs, including draft and final terms of reference and reports.

## Head of Internal Audit Opinion 2016/17

"In accordance with the requirements of the UK Public Sector Internal Audit Standards (PSIAS), 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 the follow up action from audits conducted in the previous reporting year. Due to budget constraints the programme in any year only covers a small number of areas, but over a three year period we aim to cover a broad range of governance, risk and internal control areas.

For all of the reviews undertaken in the year for which a rating was provided, we concluded that a moderate rating could be given in relation to the design and operation of controls. These reviews covered Income generation and data gathering, Information Standards, and Management of the Cyber Penetration Threat arising from moving to a cloud-based IT environment.

I am required by the PSIAS to conclude on each of Risk Management, Governance and Internal Control. Each of the reviews undertaken during the year has covered elements of each of these. However, the following reviews in particular have informed conclusions in certain areas:

- Our work on the Cyber Penetration Threat was focused on how HFEA has sought to manage one of its most significant risks in moving its IT platform to the Cloud;
- The Board Effectiveness review assessed a key component of governance; and

- Our reviews of income and information standards focused on particular internal control systems and processes.

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. Internal Audit is fully independent and remains free from interference in determining the scope of internal auditing, performing work and communicating results.

There were no high priority recommendations arising from internal audit work for us to follow-up during the year. Follow-up of medium and low priority recommendations is undertaken by management rather than by internal audit. We note that management has reported good progress in implementing agreed actions.

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

- In the case of **risk management** Moderate
- In the case of **governance:** Moderate
- In the case of **control:** Moderate

Therefore, in summary, my overall opinion is that I can give **MODERATE assurance** to the Accounting Officer that the Human Fertilisation and Embryology Authority, based on the work conducted in the year, has had adequate and effective systems of control, governance and risk management in place for the reporting year 2016/17.

*DRAFT*

*Karen Finlayson*

Head of Internal Audit

NEED TO
INSERT THE HFEA LOGO

# HUMAN FERTILISATION & EMBRYOLOGY AUTHORITY DRAFT INTERNAL AUDIT PLAN 2017/18

Government
Internal Audit
Agency

**CONTENTS**

## 1. INTRODUCTION

This document sets out the proposed Human Fertilisation & Embryology Authority (HFEA) annual Internal Audit plan for 2017/18.

## 2. HFEA CONTEXT

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

HFEA has identified its overall strategic goals as follows:

- **Setting standards – quality and safety**: improving the quality and safety of care through its regulatory activities;
- **Setting standards – donor conception**: improving the lifelong experience for donors, donor-conceived people, patients using donor conception, and their wider families;
- **Increasing and informing choice – register data**: using the data in the register of treatments to improve outcomes and research;
- **Increasing and informing choice – information**: ensuring that patients have access to high quality meaningful information;
- **Efficiency, economy and value:** ensuring HFEA remains demonstrably good value for the public, the sector and Government.

## 3. INTERNAL AUDIT POLICY, PURPOSE AND RESPONSIBILITIES

Our professional responsibilities as Internal Auditors are set out in the UK Public Sector Internal Audit Standards. In line with these requirements, we perform our Internal Audit work with a view to reviewing and evaluating the risk management, control and governance arrangements that HFEA has in place to ensure the achievement of its objectives and adds value to the organisation. This Plan also takes account of our Audit Charter and is compliant with the guidance provided in this document.

The internal audit work that we are planning to undertake during 2017/18 will be focused on governance, internal control, risk management, as well as key strategic and tactical risks faced by the HFEA.

## 4. INTERNAL AUDIT PLANNING 2017/18

### *The planning process*

To ensure that internal audit resources are used efficiently, we plan on a risk basis. Therefore, internal audit work will be closely aligned to the key risks and uncertainties pertaining to HFEA's objectives.

Audits were therefore selected using the approach outlined below:

- Review of HFEA's corporate risk register to identify corporate risks, their assurance sources and mitigating actions with a view to providing added assurance where required.
- Consulting with the Senior Management Team;
- Our knowledge of other emerging issues and intelligence gathered via audit work undertaken by PWC during the last financial years.

***Planning outcomes***

Our planning work has identified a number of risks and challenges facing HFEA. We explain below how the information gathered has been used to derive our proposals for the 2017/18 Audit Coverage Plan:

- **Table A:** Shows a summary of the draft audit reviews drawn from sources (cited above) and a proposed prioritisation of audit work. Our key criteria for prioritising areas for the 2017/18 audit plan includes:
  - key financial risks that relate to how HFEA funds are utilised
  - Particular focus on the risk management and governance to assure management of the effectiveness and efficiency of the framework in place to give sufficient, continuous and reliable assurance on organisational stewardship and the management of the major risks to organisational success and delivery of services; and
  - The robustness of data control and security.

- **Table B:** Outlines our proposed allocation of audit days against the Audit Plan for the period April 2017 to March 2018.

**The Audit and Governance Committee are invited to approve:**

- The Internal Audit Plan for 2017/18
- The associated allocation of resources in terms of days and budget.

## 5. PROPOSED AUDIT COVERAGE & AUDIT PLAN 2017/18

### 5.1 Summary of Audit Coverage

Set out below is a summary of the total coverage of the audit work proposed to be carried out within HFEA in 2017/18.

### Table A: Summary of Audit Topics

| No | Audit topic | Overview of rational and scope | Business Area | Suggested Quarter for commencement |
|---|---|---|---|---|
| 1. | **Data Loss** | This review will be undertaken to review the controls around the key risk that HFEA data is lost, becomes inaccessible, is inadvertently released or is inappropriately accessed. | Compliance & Information | • Q1 |
| 2. | **Financial Controls** | This is a standard key financial controls review. We will identify and review key financial processes and controls operated by HFEA as well as consider any potential overlaps with HTA. | Finance & Resources | • Q2 |
| 3. | **General Data Protection Regulation** | This will consider the state of preparations for the introduction of this regulation in May 2018. An audit at this stage will be useful to give assurance to the Audit and Governance Committee and to give time for any recommendations to be implemented. | Compliance and Information | • Q2 |
| 4. | **Risk Management and Governance** | Overview of general governance, risk management and assurance arrangements. Review will focus on ensuring there is a formal governance structure in place, that key risks are identified, that they are reflected accurately within | Strategy and Corporate Affairs | • Q3 or Q4 |

| No | Audit topic | Overview of rational and scope | Business Area | Suggested Quarter for commencement |
|---|---|---|---|---|
| | | the assurance framework and are a key focus for the HFEA Board. | | |
| 5. | **Follow up recommendations** | Follow up of agreed recommendations of previous audits. A summary of findings and results to be presented at each Audit and Governance Committee. | All | • Quarterly |

## Table B: Resource allocation

| Audit Area | Total Inputs (indicative days) |
|---|---|
| **Audit engagements:** | |
| **Data Loss** | 10 |
| **Financial Controls** | 10 |
| **General Data Protection Regulation** | 10 |
| **Risk Management and Governance** | 10 |
| **Follow up recommendations** | 5 |
| | 45 |
| **Other resource allocation** | |
| Head of Internal Audit and General Management | 15 |
| Advisory and consultancy | 5 |
| Contingency | 5 |
| **TOTAL** | **70** |
| **This Audit Plan is to be delivered within a budget allocation of £40,000 including VAT** | |

***SUMMARY OF AUDIT RECOMMENDATIONS***

| Year of Rec. | Category | Audit | Section | Rec # | Recommendations | Action Manager | Proposed Completion Date | Complete this cycle? |
|---|---|---|---|---|---|---|---|---|
| 2016/17 | M | DH Internal Audit | Board Effectiveness Assessment | 2 | Ensure that board members are briefed or receive alerts on key developments | Chief Executive | 30 May 2017 | √ |
| | L | | | 3 | Consider developing additional training and support for new board members | Chief Executive | 30 May 2017 | √ |
| | M | | Information Standards | 5 | Per HFEA guidance, an evidence source, i.e. a staff member with appropriate knowledge and expertise, is not required to formally approve the draft publication | Head of Engagement | 1 April 2017 | √ |
| | L | | | 6 | Lack of written evidence of approval from the Head of Engagement and/or a Director for six of the eight publications selected for testing. | Head of Engagement | 1 April 2017 | √ |
| | L | | Cloud Cyber Risk Assessment (advisory) | 8 | Business Continuity - divergent route network connectivity | Head of IT | 30 April 2017 | √ |
| **TOTAL** | **1** | | | | | | | |

| FINDING/*RISK* | Recommendation | Agreed actions / Progress Made | Owner/Completion date |
|---|---|---|---|
| **2016/17 – INTERNAL AUDIT CYCLE** | | | |
| **BOARD EFFECTIVENESS SELF-ASSESSMENT** | | | |
| **1. Ensure that board members are briefed or receive alerts on key developments** | | | |
| Interviews with the board members identified that some members felt that there were some gaps in the sharing of information between the board meetings, especially for those board members who are not involved in the work of the Authority's committees. In particular, the board members noted that where the Authority is involved in legal cases, the members would welcome receiving updates before the cases become public knowledge through the media.<br><br>In addition, while it was reported that the working papers provided for the board include the right level of detail and also an update on previously agreed actions, a few comments were received about providing board members with clearer updates on the progress, completion of agreed actions and implementation of policies, especially where the implementation may be over a longer period of time.<br><br>Without clear and timely updates, board members may not have full visibility of current cases and legal challenges to the Authority's decisions. This may impact on how they respond when matters that have reached the public domain are raised with them.<br><br>Board members may also lack visibility on the rate of progress and completion of actions and implementation of decisions, which could impact on their ability to hold the Executive team to account for timely progression and implementation. | Ensure that board members are briefed or receive alerts on any key developments, including decisions and legal cases, on a timely basis to help prepare them for any questions that may arise.<br><br>Ensure that updates on progress and implementation of agreed actions and policies provide a full summary of progress made, next steps and, where relevant, an indication of whether progress is in line with the original timetable and if the originally intended completion date should be achieved. | We recognise that the part time nature of Board members' role does not always allow them to keep up to date with key developments. We currently do a number of things to address this - weekly press updates, private legal updates, regular briefing meetings between Chair, Deputy Chair, Chair AGC and Chief Executive – but accept that we may need to do more. We will ask members what additional information they would find most useful.<br><br>We will consider how the strategic performance report might encompass an action log (or similar) to capture progress over time.<br>**May 2017 update**<br>Discussed with Authority members on 10 May will take further actions in light of any comments we may receive.<br><br>**Recommendation complete** | ***Chief Executive***<br><br>**30th May 2017**<br><br>**COMPLETE** |
| **2. Consider developing additional training and support for new board members** | | | |
| Positive feedback was received in respect of the legal training provided as part of the induction for new board members. However, some further induction training on corporate governance and the board's operational framework would be welcomed.<br><br>Some members would welcome more training and development support around the role of the board members and specifically their responsibilities and work expectations outside of meetings. Further discussion with the Chair and the Chief Executive confirmed that conversations about the role, responsibilities and work expectations are held informally with the new board | Consider developing additional training and support for new board members around the operation of the board, corporate governance and providing additional guidance on being an | Chair and Chief Executive currently provide informal induction and support for new members, alongside formal legal training. We will discuss with members what more formal corporate induction would be most helpful<br><br>**May 2017 update**<br><br>As above. | ***Chief Executive***<br><br>**30th May 2017**<br><br>**COMPLETE** |

| | | | |
|---|---|---|---|
| members. However, formalisation of those discussions in a more structured training approach may assist clarity about the board members' role, and could include more clarification of the expectations between board meetings.<br><br>New board members may lack clarity on how the board operates, its decision making processes and what is expected of board members, particularly between meetings. If this was to be the case, board and individual effectiveness could be impaired, and this may be particularly relevant at times of change in board membership. | effective board member, including activities between board meetings. | **Recommendation complete** | |
| **INFORMATION STANDARDS** | | | |
| **3.** | **Per HFEA guidance, an evidence source, i.e. a staff member with appropriate knowledge and expertise, is not required to formally approve the draft publication** | | |
| The 'Producing corporate website content' guidance document, requires that the communications team works with an evidence source to gain the facts that they need to update or create content and decide on timelines for the information to be produced. The evidence source is usually a member of staff with the relevant knowledge and expertise.<br><br>However, it is not required that the evidence source formally approves the publication to verify the factual accuracy prior to release. From our testing we noted that for six out of the eight publications tested, there was written approval from the evidence source, which indicates that this is occurring in practice in some cases, but we also noted two documents where formal approval was not obtained. The two publications for which we were unable to obtain evidence of written approval from the evidence source were 'Our partners' and 'Applying to use our data for research'. Management confirmed that verbal approval was provided for the 'Our partners' page and for 'Applying to use our data for research', we did see evidence of working with the evidence source, although not final approval.<br><br>As the corporate information contained on the website can vary in the risk attached to any inaccuracies, the requirement for review and approval by the evidence source could be applied on a risk based approached, taking into account the type of information being published.<br><br>*The information provided could be of poor quality and/or inaccurate which could undermine HFEA's stated objective of building trust in their regulation. Furthermore, if the evidence source does not sign off the publication there might be a lack of accountability should the publication prove to be inaccurate.* | Consideration should be given to require evidence sources to provide formal approval of each publication.<br><br>As the corporate information contained on the website can vary in the risk attached to any inaccuracies, this requirement could be applied on a risk based approached, taking into account the type of information being published.<br><br>The guidance document should be updated for any changes to policy. | We acknowledge this and agree with the recommendation.<br><br>***We will amend the guidance document so that evidence sources must formally approve any changes.***<br><br>**May 2017 update**<br><br>The guidance document – producing corporate information has been amended to include guidance that in some cases the information source must formally approve the final information.<br><br>**Recommendation complete** | ***Head of Engagement***<br><br>1 April 2017<br><br>8 May 2017<br><br>**COMPLETE** |

| 4. | Lack of written evidence of approval from the Head of Engagement and/or a Director for six of the eight publications selected for testing. | | |
|---|---|---|---|
| The guidance document requires that corporate publications are subject to appropriate review before release. This includes a final sign off from a Director and/or by the Head of Engagement.<br>During our review we were unable to locate evidence of formal written approval for six publications. In discussion with the Head of Engagement it was stated that verbal approval was provided on each of these occasions and, therefore, this is considered a documentation issue. The publications for which we were unable to review evidence of approval were:<br>1) Our committees and panels<br>2) Our partners<br>3) Making a complaint about a fertility clinic<br>4) Meet our Authority members/our board<br>5) Applying to use our data for research<br>6) Home Page<br><br>*As the public has access to the new website there is a risk that inaccurate information could be published which could undermine HFEA's stated objective of building trust in their regulation if appropriate review has not been undertaken. In addition, if the publications were of poor quality this might lead to confusion amongst users which may lead to higher levels of individual requests for help and/or guidance, impacting use of resources. If approval is not evidenced, there is greater risk that a publication may be released which has not been appropriately reviewed and approved, which increases these risks.* | All approvals should be in writing to evidence that all publications have been appropriately reviewed and approved, and have a complete audit trail. | We acknowledge this and agree with the recommendation.<br><br>***We will clarify the guidance and ensure an email is sent to the author to confirm approval***<br><br>**May 2017 update**<br><br>The guidance says that the approver must always send an email to the author approving the information. This must be recorded in TRIM and referred to in the information production spreadsheet.<br><br>**Recommendation complete** | ***Head of Engagement***<br><br>1 April 2017<br><br>8 May 2017<br><br>**COMPLETE** |

## CLOUD CYBER RISK ASSESSMENT (ADVISORY)

| 5. | Business Continuity (Advisory) | | |
|---|---|---|---|
| Using a public cloud service such as Microsoft's Azure Cloud requires a network connection to the outside world (internet). A network related incident at the HFEA office could result in staff being unable to access key services hosted on the Azure Cloud | We recommend HFEA to update their Business Continuity policies to ensure it has appropriate plans and procedures in the event of an incident, such as network failure impacting services hosted on the Azure Cloud. This could be something simple as allowing staff to work from a secure environment such as their home via a secure VPN connection. | Agreed. IT staff can already access Azure services from remote locations. General HFEA staff can access Office 365 from home.<br><br>***Remote access in place.***<br><br>We will investigate divergent route network connectivity for Spring Gardens. ***Divergent route to be investigated***<br><br>**May 2017 update**<br>The HFEA has a second wireless connection that can be used in the event of primary internet connectivity failure.<br>**Recommendation complete** | ***Head of IT***<br><br>***Complete***<br><br>***by end of April 2017***<br><br>**COMPLETE** |

# Information for Quality programme: update

| | | | |
|---|---|---|---|
| **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 (13/06/2017) 549 NJ | | |
| Meeting date | 13 June 2017 | | |
| Author | Nick Jones, Director of Compliance and Information | | |
| **Output:** | | | |
| For information or decision? | For information | | |
| Recommendation | The Committee is asked to Note:<br>• The HFEA Website GDS live assessment takes place on 7th Jun 2017<br>• Progress on the new data submission system<br>• The progress with data migration and assurance, and receive a presentation from Northdoor plc on project assurance<br>• Budget update and spending to date<br>• Updated risks and issues | | |
| Resource implications | The IfQ Programme budget has now been expended. The budget for remaining work has been established at £350,000 | | |
| Implementation date | During 2017–18 business year | | |
| Communication(s) | Regular, range of mechanisms | | |
| Organisational risk | ☐ Low | ☐ Medium | ☒ High |
| Annexes: | None | | |

# 1. Background

**1.1.** The Information for Quality (IfQ) programme encompasses:

- The redesign of our website and Choose a Fertility Clinic (CaFC) function
- The redesign of the 'Clinic Portal' (used for interacting with clinics) and combining it with data submission functionality (Release 2) that is currently provided in our separate system (used by clinics to submit treatment data to us)
- A revised dataset and data dictionary which will be submitted for approval by the Standardisation Committee for Care Information (SCCI)
- A revised Register of treatments, which will include the migration of historical data contained within the existing Register
- The redesign of our main internal systems that comprise the Authority's Register and supporting IT processes.

**1.2.** This paper updates Members on:

- Completing the programme
- Work in progress
- Programme budget
- Risks and issues

# 2. The IfQ programme

**2.1.** Given the importance of IfQ to our strategy, we update the Committee on progress at each meeting. It has been agreed by the Authority that the Programme will close, and we can start to assess the expected benefits, but only at the point at which the new HFEA website is launched. Thereafter we will continue to report on the completion of the treatment data submission system, and associated infrastructure.

**2.2.** This paper sets out the path to conclusion of the Programme and then of the residual work. The programme is progressing per 'agile' principles required by the Government Digital Service (GDS).

**2.3.** Our attention is now focussed on completing the work necessary to move the HFEA website from Beta to live; and, concurrently, producing a Beta version of the treatment submission system (located in the HFEA Clinic Portal, launched in January 2017).

# 3. Work in progress

### HFEA Website and choose a fertility clinic

**3.1.** The Government Digital Service provided feedback in early May 2017 to be addressed before we can proceed 'to live'. This included the necessity of thorough security penetration testing; the completion of an exercise and report as to the accessibility of the

website to all users; and confirmation of our arrangements for continual improvement, and active management, of the website.

**3.2.** The required work to satisfy GDS standards has now been completed and an assessment by GDS was expected to take place in May 2017. The assessment is now taking place on 7 June 2017 – with an update provided at the meeting. It is possible the website will have been launched.

### Release 2 – data submission component

**3.3.** This project is picking up speed following the focus on the website, and the Portal before that. Very good progress is being made on the 'front end' experienced by users and we have begun sharing the outputs of this with users. This work will yield benefits in terms of both making user interaction more friendly and provide greater flexibility to incorporate more complex submission elements. Similarly, engagement with clinics' suppliers of patient record systems is ongoing and positive.

**3.4.** That said, there is much to do, and we continue to need the support of externally commissioned expertise (contracted in developers) to progress. Our plan to release the new system to current 'EDI' users remains September 2017.

### Register data migration

**3.5.** As reported regularly, over the last 12 months, the Register has been subject to a thorough overhaul, and cleansing exercise – in preparation of migration of the data to a new Register to enable all the benefits of the data submission system to be realised.

**3.6.** Data Migration is progressing at a slow pace following the focus of resources on other activities within the organisation; this includes greater emphasis on the website (CaFC) and the transfer of knowledge from staff leaving the organisation to colleagues, some of whom are involved in the data migration effort.

**3.7.** Nevertheless, the goal of completing a significant milestone relating to the data migration – the third 'trial load' is on track for completion in July 2017.

**3.8.** Members will recall we have appointed a third party (Northdoor plc) to provide assurance that we are compliant with our own data migration strategy – commissioned in 2015/16. Northdoor has now completed its second data migration audit. It is timely for Members to be appraised of the findings of this audit - to receive information about the findings and provide an opportunity for questions and any areas of reassurance that the Committee may find useful, here or at a future date. **A senior representative from Northdoor will present the findings of their review at the meeting.**

## 4. Programme budget

**4.1.** The IfQ programme budget has now closed; with final expenditure (subject to final accounts) of £1.276m compared to our planned programme budget of £1.227m. That expenditure includes substantial work (to end March 2017) on the data submission project, although, as noted above, there is a considerable amount of work still to complete.

**4.2.** The budget for completion of the data submission project has been established at £350,000 for the 17/18 financial year. The budget is in line with capital expenditure expectations. As such expenditure is on investment, or development, of the IT system estate – in essence development expertise provided by contractors on short-term contracts, and some programme management resource (delivered by internal secondee).

| Budget this F/Y | Planned spend | Actual to date | Monthly Variance |
|---|---|---|---|
| £350,000 (17/18) | £40,000 (April 17) | c. £37,700 (awaiting finance nominal report) (April 17) | c. £2,300 |

## 5. Risks and issues

**5.1.** Risks are reviewed regularly, the latest review on 12 May 2017 and several new risks to the project were identified. The main area of risk relates to staffing, particularly given the departure of colleagues from the organisation further to the organisational change programme.

**5.2.** The top five risks to the project have been identified as:

- Increasing workload and lack of resources
- Loss of knowledge within the IT team
- Data migration supported by only a few people, often diverted to other work
- Reliance on external contractors, which means there is a risk of contractors leaving at short notice
- Key IT knowledge will soon be transferred to contractors

**5.3.** Mitigation in place:

- Recent experience of recruiting a developer has made us more aware of the risks we may run into in the absence of existing knowledge, or high quality documentation. Risks are largely cost related further to the necessary learning curve as external contractors will need more time to understand the architecture, code, systems etc. currently being used. Mitigating this risk will require dedicated time and resources on knowledge transfer and handover, as well as a structure for technical documentation.
- We are currently in the process of recruiting a further developer to overlap with the current lead developer to cover the transition period pending recruitment of a permanent member of staff.

## 6. Recommendation

The Committee is asked to note:

- The HFEA Website GDS live assessment takes place on 7th Jun 2017
- Progress on the new data submission system

- The progress with data migration and assurance, and receive a presentation from Northdoor plc on project assurance
- Budget update and spending to date
- Updated risks and issues

# Cyber security

| | | | |
|---|---|---|---|
| **Strategic delivery:** | ☒ Setting standards | ☒ Increasing and informing choice | ☒ Demonstrating efficiency economy and value |
| **Details:** | | | |
| Meeting | Audit and Governance Committee | | |
| Agenda item | 11 | | |
| Paper number | AGC/(13/06/2017) 551 | | |
| Meeting date | 13 June 2017 | | |
| Author | Karl Saunders, System Support Analyst | | |
| **Output:** | | | |
| For information or decision? | For information | | |
| Recommendation | The Committee is asked to note this report. | | |
| Resource implications | No additional resources, costs incurred within IfQ programme or business as usual expenditure | | |
| Implementation date | Ongoing | | |
| Communication(s) | Ongoing | | |
| Organisational risk | ☐ Low | ☒ Medium | ☐ High |
| Annexes | None | | |

## 1. Introduction and summary

**1.1.** Cyber security risks have gained a lot of attention in the media due to the recent malware attacks. This has led to a loss of reputation and possible loss of data.

**1.2.** Malware attacks that recently impacted the NHS trusts have been prevalent for some time. The story behind these malware attacks are very characteristic of any successful cyber-attack, whereby the hackers focus on using known vulnerabilities and then betting on the fact that organisations don't know how to fix what matters.

**1.3.** This paper sets out to highlight the risks to our organisation, the steps taken to mitigate our exposure to this type of risk and some recommendations with regards to our vulnerabilities. It concludes with a discussion on some 'big' questions we should ask ourselves in the light of the prominence of cyber-threat.

## 2. Cyber-attack overview

**2.1.** The recent "WannaCry" cyber-attack is estimated to be the largest attack yet, with more than 300,000 organisations in more than 200 countries falling victim. This attack exploited a known vulnerability in Microsoft windows SMB server, which Microsoft had provided a fix for in March 2017. Unfortunately, many organisations had not applied this fix or were simply running operating systems that had reached their end of life (Windows XP, Windows server 2000) and so no longer received these security fixes. This created the vulnerability for the hackers to exploit.

**2.2.** The type of malware attack on the NHS is a very general attack so will focus on a known vulnerability. However, no organisation can guarantee the security of its systems against a determined external attacker or internal leaker. Some forms of cyber vulnerabilities can be instigated knowingly or unknowingly from inside the organisation.

**2.3.** Cyber-attacks are ever changing and can come in many varied forms, with the latest being a focus on hiding a virus within software, it then uses the user's internet browser to steal credentials, download further viruses onto the users' device.

**2.4.** Another form of cyber-attack can take the form of a compromised web site. This is where a hosted website has been hacked, the hacker will infect a webpage on the site which could either redirect you to another site managed by the hacker and emulate a recognised logon system, enabling the hacker to steal your credentials or tricking you into downloading more viruses.

**2.5.** A question often asked by those seeking assurance as to vulnerability, is 'I understand the potential for attack, how many attacks have we had, and therefore defended ourselves against?' This is impossible to answer – or at least it would involve disproportionate effort to be able to provide a realistic assessment. Our systems prevent hundreds of emails with attachments and links – some or all potentially injurious – from entering the system in a week. Section 3. Addresses what we do to mitigate the risks, and Section 4. seeks to widen the narrative so that leaders and boards are making effective challenges.

## 3. HFEA mitigations of cyber risks

**3.1.** With the introduction of our new desktop estate replacing our Windows 7 machines with the latest Microsoft operating system of Windows 10 we have been able to implement a more robust device management method by deploying Microsoft InTune. This enables us to manage the deployment of fixes from Microsoft to our end users at the earliest opportunity reducing our exposure to these types of risks. InTune also enables us to enforce device policies to mitigate the risks of cyber-attacks. Finally, InTune also enables us to manage the deployment of antivirus software on each end user's device and schedule regular scans of the device.

**3.2.** In much the same way, we have in place a Microsoft systems management server that manages the patch deployment to our in-house server estate. This is carrying out the patch and virus updates on our 'on premise' infrastructure that InTune is carrying out for out desktop environment.

**3.3.** The HFEA has a robust backup strategy that that backs up data to two different types of media and we are currently testing a third type of cloud based backup strategy.

**3.4.** With the deployment of office 365 we have introduced access to cloud storage in the form of OneDrive. This ensures our end users are not saving HFEA data on their local devices, with the possibility of data loss through either a cyber-attack on the individual's device or in the event of a device failure.

**3.5.** Legacy systems have been either upgraded to more modern operating systems or retired from service and the IFQ programme has also enabled us to deploy parts of our infrastructure into the Azure cloud environment. This cloud approach has significant additional security benefits as part of a managed service.

**3.6.** Attacks can come in many different forms, infected email, infected removable devices, bundled in with other software and hacked/compromised websites. Some of the greatest weakness in securing a system will be the user interaction with the system. Therefore, it is imperative that all our users know and understand their role in securing both our systems and our reputation. It is paramount that we have a clear and continual message of vigilance with regards to cyber risks. The danger with some of this communication can be that it is often something that is repetitive and can be seen in itself as a form of spam, an irony in itself. The challenge is to keep this information sharing in a relevant and clear way that engages our staff.

## 4. Questions to ask ourselves

**4.1.** It is clear that the operational consequences for organisations affected by an attack are potentially enormous. Running alongside this are the reputational risks. Civil Service World, in the light of the recent attack, has set out some useful pointers for public leaders.

**4.2.** 'It is easy to blame this crisis on some hapless leader who saved money by ending support for XP. But that is like attributing an air crash to 'pilot error', as was normal 30 years ago. Stanley Roscoe, an aviation psychologist of the time, described such

conclusions as “the substitution of one mystery for another”. He thought aviation investigators could do much better. They did and so should we.’

**4.3.** The piece goes on to contrast the civil service being full of intelligent, well-intentioned people, with humans - who are ‘predictably irrational’ and seeing this as both a strength and weakness. We know that people are every organisation’s greatest assets and its greatest risks. It is argued that leaders must understand *behavioural* and *organisational* risks and how to manage them effectively

**4.4.** ‘Persistently digging to root causes typically reveals an unseen web of human weaknesses that can lie latent, incubating for years – until luck runs out, when they cause a crisis.’ The risk indicators include

- internal silos;
- professionals who saw this coming but were not heard;
- gaps in leadership skill and experience;
- leaders resistant to unwelcome news;
- decision-makers who neither understood IT nor sought explanations;
- inability to learn from history and minor failures;
- incentives that undermine the system’s integrity;
- communication failures;
- cultural weaknesses, complacency and complexity.

These risks are not, of course, limited to cyber-security risks. This paper provides assurance on some of these indicators. In considering our overall appraoch to the management of risk within the HFEA the Committee may have a view on others.

The Executive’s assessment is that we do not display these features, but are alive to each and there is no room for complacency.

## 5. Recommendation

**5.1.** The Audit and Governance Committee is asked to:

- Note this report
- Comment on the risk indicators at 4.4

# Resilience and Business continuity

| | | | |
|---|---|---|---|
| **Strategic delivery:** | ☒ Setting standards | ☒ Increasing and informing choice | ☒ Demonstrating efficiency economy and value |
| **Details:** | | | |
| Meeting | Audit and Governance Committee | | |
| Agenda item | 12 | | |
| Paper number | AGC (13/06/2017) 552 | | |
| Meeting date | | | |
| Author | Nick Jones, Director of Compliance and Information | | |
| **Output:** | | | |
| For information or decision? | For information | | |
| Recommendation | The Committee is asked to note this report. | | |
| Resource implications | As outlined | | |
| Implementation date | Ongoing | | |
| Communication(s) | Ongoing | | |
| Organisational risk | ☐ Low | ☒ Medium | ☐ High |
| Annexes | | | |

## 1. Introduction

**1.1.** This paper provides an update on our arrangements for business continuity, for preparing and managing our activity in the event of loss of staff, information technology support, office accommodation. This follows a discussion at the last meeting of the Committee in March 2017 where we reported on a test of our emergency alert system (which sends text messages to all members of staff), and the poor response rate that resulted. The Committee requested a further report.

**1.2.** The HFEA has Business Continuity Plan and a Pandemic Response Plan in place and named staff have responsibilities. Business continuity has a dedicated site in Microsoft Office 365 (a web-based portal where business systems can be accessed with a log-in id and password) where an up to date copy of the Business Continuity Plan and other key documents are made available. All HFEA staff have access to this facility.

## 2. Effectiveness

**2.1.** Following the test of the emergency alert system a review was undertaken primarily by surveying staff on their awareness of the arrangements and their experience of using it. The headlines are as follows:

- Only three members of staff reported not receiving the text message saying that business continuity arrangements had been invoked as a test – and that the instruction was to log on to the O365 business continuity page and leave a message of confirmation
- However, only just over a third of staff could log on to O365 without problem and leave a message
- Of those, most could access the BCP page – but a few (4) could not, suggesting it was not clear to those staff members how the page could be accessed.

**2.2.** From this test, it can be concluded that while the arrangements for notifying staff of an incident broadly work (although there are a few issues relating to our holding up to date contact details), there is a significant problem in accessing the BCP site.

**2.3.** The importance of the site cannot be overstated. The site will be our principal communication channel in any emergency situation and will provide a means by which we can update staff on the status of any incident or interruption to arrangements for business as usual. It will also provide the ability to enable access to (some) corporate files, personal work-related files and email and communications facilities. In other words, the site is the place where business continuity happens.

**2.4.** Further analysis reveals three main problems relating to logging on (together with several individual-specific issues):

1) The user name and password combinations did not work - there is a slightly different sign-in protocol between desktop log-in and O365 sign-in and too many staff were not aware of this.

2) There were compatibility and log-in issues between phones and the O365 site - the text arrived in the evening (obviously) and many staff attempted to use their smartphone to log-in (either personal 'phones or HFEA issue). Around half of staff using phones could not access the site, partly because of compatibility issues and partly log-in difficulties

referenced above. The issues were equally distributed whether the phone was personal or HFEA issue.

3) Staff did not have their HFEA issue laptop at home (it is not a requirement that they do) which should be more reliable - that said, some staff with personal PCs and tablets, could log-in and the 'phone related issues were not apparent.

**2.5.** Clearly this is not a satisfactory situation. However, the very process of going through the exercise and the subsequent survey of staff has raised awareness of both the BCP and the arrangements necessary for accessing O365, together with the business continuity site.

**2.6.** Many staff have now resolved log-on and password difficulties. In addition to that we have worked (mainly on a one-to-one basis) with colleagues to resolve some of the phone-related issues.

**2.7.** Nevertheless, this reactive activity needs to be supplemented with a formal and planned set of actions.

## 3. Actions

**3.1.** We are taking several obvious actions to embed BCP awareness and enable straightforward access. Ideally we would have liked to be at the stage where we had implemented these actions but due to a range of factors this has slipped a little. These actions include:

i. Completing an awareness raising communication exercise for current staff. That is a clear set of instructions and advice that staff will sign having received. We expect managers to be responsible for confirming their teams are aware of their obligations relating to business continuity.

ii. Ensure that the BCP pages are 'device agnostic' – that is wherever and however staff need to access the site they can. This will entail some tweaks to the site and clearer instructions, as part of the above.

iii. We have introduced a good process for staff joining the HFEA about their awareness of O365, the BCP pages, and the importance of keeping contact details up to date. A process is in place for leavers such that the BCP staffing list is continually updated. Only HFEA staff/members must be able to access the site.

iv. Now that all Members have access to O365 we will need to roll out BCP arrangements so that Members are integrated to business continuity arrangements.

**3.2.** We aim to complete this work by the end of June 2017.

## 4. Next steps

**4.1.** What has become much clearer over the last few months in considering the plan is the benefits of O365 as an operating system and the potential opportunities it might provide in terms of business resilience on a range of fronts – not just when there is an emergency. In short, the HFEA, could operate as a virtual entity moving the focus away from business continuity to how the HFEA business model promotes efficiency and effectiveness.

**4.2.** The exercise for considering this should clearly not be mediated through the BCP process. The HFEA strategy sets the vision for us, and the way the HFEA is structured (following the organisational change programme) provides the foundations for this – for example, the

establishing of the Chief Information Officer function; a systems management team focused on resilience and business continuity; an information governance specialism and so on.

**4.3.** While we will want to take the opportunity to review the BCP over the next few months both in the light of those changes and the technological opportunities available to us, this work will not take our focus from taking the actions set out in section 3 above.

## 5. Recommendation:

**5.1.** The Audit and Governance Committee is asked to note:

- that a series of actions are underway to improve the business continuity arrangements
- that longer term the Business Continuity Plan itself will be reviewed in the light of experience and the organisational change underway.

# ALB risk interdependencies

| | | | |
|---|---|---|---|
| **Strategic delivery:** | ☒ Safe, ethical effective treatment | ☒ Consistent outcomes and support | ☒ Improving standards through intelligence |
| **Details:** | | | |
| Meeting | Audit and Governance Committee | | |
| Agenda item | 13 | | |
| Paper number | [AGC (13/06/2017) 553 PR] | | |
| Meeting date | 13 June 2017 | | |
| Author | Paula Robinson, Head of Planning and Governance | | |
| **Output:** | | | |
| For information or decision? | Information and comment. | | |
| Recommendation | AGC is asked to note the information in the paper about the DH's guidance on identifying and managing system risk interdependencies, the HFEA's proposed approach, and the annexed DH guidance note. | | |
| Resource implications | In budget. | | |
| Implementation date | Ongoing. | | |
| Organisational risk | ☒ Low | ☐ Medium | ☐ High |
| Annexes | Annex: DH guidance – Management of risk interdependencies in the health and care system (for Executive Summary see p3-4 of the Annex) | | |

# 1. System risk interdependencies

**1.1.** A 2016 internal audit report for the Department of Health identified risk interdependencies between DH and its ALBs as a potential area of weakness in the risk management system.

**1.2.** Since that time, the Department has been discussing risk interdependencies with ALB risk leads (who meet as a Network Group, hosted by DH, several times per year).

**1.3.** There have been two main products from this work:

- DH guidance on the management of risk interdependencies (see Annex A)
- A workshop (in February 2017) for all ALBs to share information about risk interdependencies.

**1.4.** DH's intention is to produce and share a matrix capturing the interdependencies that were identified at the workshop. Pending production of that document, this paper sets out some of the main points and themes.

**1.5.** We have also incorporated risk interdependencies into our risk register so that these are clearly set out on a separate line. This will make it easier to identify any needed actions, and to report back to the Department as and when necessary.

# 2. Risk interdependencies workshop

## The workshop

**2.1.** The workshop took place on 28 February 2017, and was attended by various DH staff and risk leads from all the health ALBs.

**2.2.** The NHS ALBs shared a strong focus on a number of particular risk areas, with many already-recognised interdependencies between them, or with the Department. Such risks included funding and NHS savings, the Comprehensive Spending Review in 2019/20, and IT and information security risks. These ALBs already have a number of collaborative arrangements in place for risk interdependency management across the NHS, and are looking to work more closely with the Department, and perhaps to automate some of their group risk tracking.

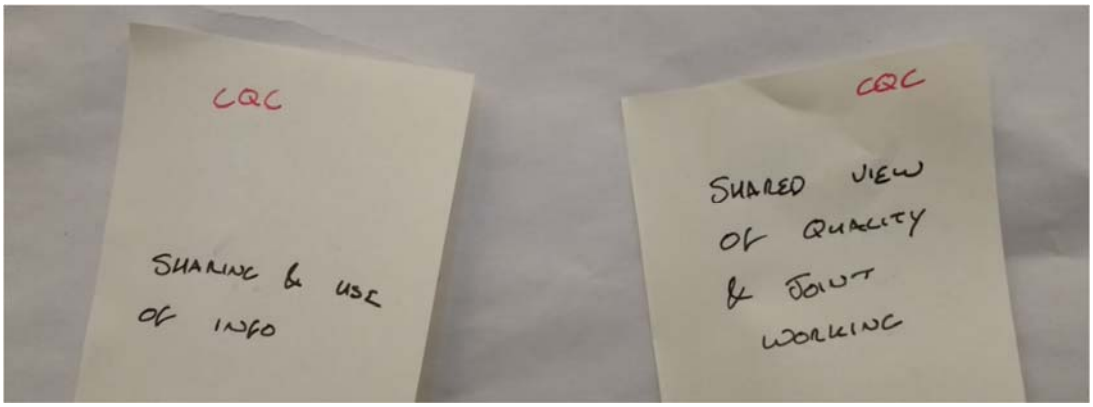
**2.3.** Despite the larger size and complexity of the majority of organisations represented, their approach to risk management is the same as ours – they have a strategic risk register with operational and project risk logs underneath. They use the Treasury's 'Orange Book' as their general guide, with the same definitions of inherent and residual risk, and most use the same 1-5 scoring system as us.

## Outcomes

**2.4.** A number of common themes were evident:

- Money (amount of, management of, associated reputational risks)
- Workforce (retention, pay, skills).
- Legislative and political change
- Cyber security
- Brexit consequences

**2.5.** Our own main risk interdependencies are with the Department – on things like our legislation, our funding, and sometimes policy or media matters. The only interdependencies identified with us came from the CQC, who added two shared risks to every ALB's risk sheet during the workshop. However, these were about sharing information, and defining quality. Most delegates saw these as collaborative working interdependencies, rather than risk interdependencies, and no particular risk was specified in relation to the HFEA. We believe our working relationships and memorandum of understanding with the CQC enable us to manage any shared or overlapping regulatory risks as and when they arise.




**2.6.** In discussion, it was clear that the biggest two common risk areas are financial risks and workforce challenges. Data sharing, cyber security and complex, multi-layered central Government approval and reporting processes were also frequently mentioned.

## Next steps

**2.7.** We agreed:

- To continue to share information about our biggest common risks at each subsequent ALB Risk Network meeting.
- To feed back to our audit and risk committees about the workshop.
- To discuss any new risk interdependencies identified through the workshop with the relevant organisations, so as to ensure a joint mitigation plan is in place. (For us, the interdependent risks we have with the Department are already regularly discussed and well controlled.)
- To review our risk registers with this session in mind, and incorporate interdependencies into the structure of our risk registers.
- That the Department would circulate all the identified interdependencies in due course.

**2.8.** We also agreed that good relationships and dialogue were more important for managing risk interdependencies than words in a risk register. Collaborative relationships should be active and responsive, with associated agreements up to date, so that account can be taken of risk (and other) interdependencies whenever there is joint working.

## 3. Recommendation

**3.1.** AGC is asked to note the above report, and the annexed DH guidance.

**3.2.** Comments are welcomed – either on this paper, or on the interdependencies listed in the revised risk register (the next item on the agenda).

# Strategic risks

| | | | |
|---|---|---|---|
| **Strategic delivery:** | ☒ Safe, ethical effective treatment | ☒ Consistent outcomes and support | ☒ Improving standards through intelligence |
| **Details:** | | | |
| Meeting | Audit and Governance Committee | | |
| Agenda item | 14 | | |
| Paper number | [AGC (13/06/2017) 554 PR] | | |
| Meeting date | 13 June 2017 | | |
| Author | Paula Robinson, Head of Planning and Governance | | |
| **Output:** | | | |
| For information or decision? | Information and comment. | | |
| Recommendation | AGC is asked to note the latest edition of the risk register, set out in the annex. | | |
| Resource implications | In budget. | | |
| Implementation date | Strategic risk register and operational risk monitoring: ongoing.<br><br>CMG reviews risk quarterly in advance of each AGC meeting.<br>AGC reviews the strategic risk register at every meeting.<br>The Authority reviews the strategic risk register periodically. | | |
| Organisational risk | ☐ Low | ☒ Medium | ☐ High |
| Annexes | Annex 1: Strategic risk register | | |

# 1. Strategic risk register

## Latest review

**1.1.** CMG reviewed a draft of the new risk register at its meeting on 17 May. Following the launch of our new strategy for 2017-2020, the risks have been considered afresh.

**1.2.** We recognised that there are a number of core (but high level) risks that constitute risks to the delivery of the strategy as a whole (financial risks, legal challenge, cyber-security, people risks, and change), while other risks relate to specific elements of the strategy. We believe this is a valid and useful distinction, and have grouped the new risks accordingly.

**1.3.** We have also revised the format for recording risks, making more prominent the risk itself and the tolerance level. Many of the risk sources and controls listed in the previous edition of the risk register are still applicable, and have therefore been carried across. We have added a new section on risk interdependencies with other ALBs or the DH. And we have moved all the methodological material to the back of the report.

**1.4.** CMG's initial comments on the new risk register are summarised towards the end of the annex, in the 'reviews and revisions' section.

**1.5.** Since several risks are new, the usual graphical overview of residual risks plotted against risk tolerances has been omitted this time. We will resume this from the next meeting.

**1.6.** Two of the seven risks are currently above tolerance.

**1.7.** For the time being we have a total of five generic risks and two strategy-specific risks. I would expect the new risk register to develop over the next few reviews, and the Committee's comments and observations will help to shape it further.

# 2. Recommendation

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

# Strategic risk register 2017/18

## Risk summary: high to low residual risks

| Risk area | Strategy link* | Residual risk | Status | Trend** |
|---|---|---|---|---|
| LC1: Legal challenge | Generic risk – whole strategy | **15 – High** | Above tolerance | ⇔⇔⇔⇧ |
| OC1: Organisational change | Generic risk – whole strategy | **12 – High** | Above tolerance | -⇧ |
| C1: Capability | Generic risk – whole strategy | **12 – High** | At tolerance | ⇔⇧⇔⇔ |
| FV1: Financial viability | Generic risk – whole strategy | **9 – Medium** | At tolerance | ⇔⇔⇔⇔ |
| CS1: Cyber security | Generic risk – whole strategy | **6 – Medium** | At tolerance | **New** |
| RE1: Regulatory effectiveness | Improving standards through intelligence | **6 – Medium** | At tolerance | **New** |
| ME1: Effective communications | Safe, ethical effective treatment<br>Consistent outcomes and support | **6 – Medium** | At tolerance | **New** |

* Strategic objectives 2017-2020:

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

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

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

Consistent outcomes and support: Improve access to treatment

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

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

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

Old risk register 2014-2017: Authority 16 November ⇨ CMG 23 November/AGC 7 December ⇨ CMG 8 February

New risk register 2017-2020: CMG 17 May 2017

(Some risks are new or recent, as at May 2017, and therefore do not yet show four trend points.)

## 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 | **9** | **9** | **9 - 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 |
|---|
| **At tolerance.**<br>As of May 2017 we are within budget. It is too early to forecast what our position will be at the key quarter-end. Detailed analysis work on treatment fee income will commence in Q3 of this financial year. |

| Causes / sources | Mitigations | Timescale / owner |
|---|---|---|
| Our annual income can vary significantly as:<br>- Our income is linked directly to level of treatment activity in licensed establishments<br>- Forecasting treatment numbers is complex<br>- We rely on our data submission system to notify us of billable cycles. | Activity levels are tracked and change is discussed at CMG, who would consider what work to deprioritise and reduce expenditure. | Monthly (on-going) – Richard Sydee |
| | Fees Group enables dialogue with sector about appropriate fee levels. | Ongoing – Richard Sydee |
| | We have sufficient reserves to function normally for a period if there was a steep drop-off in activity, or clinics were not able to submit data and could not be invoiced. If this happened, resolving it would be high priority, and the roll-out of the new data submission system will be planned carefully. | In place – Richard Sydee/Nick Jones |
| | Worked planned in 2017/18 to better understand the likely future trends in treatment cycle activity. | Being planned – Richard Sydee |
| Annual budget setting process lacks information from directorates on variable/additional activity that will impact on planned spend. | Annual budgets are agreed in detail between Finance and Directorates with all planning assumptions noted. Quarterly meetings with Directorates flags any shortfall or further funding requirements. | Quarterly meetings (on-going) – Morounke Akingbola |

| | | |
|---|---|---|
| Project scope creep. | Senior Finance staff present at Programme Board. Periodic review of actual and budgeted spend by IfQ project board and monthly budget meetings with finance. | Ongoing – Richard Sydee or Morounke Akingbola |
| | Cash flow forecast updated. | Monthly (on-going) – Morounke Akingbola |
| **Risk interdependencies (ALBs / DH)** | **Control arrangements** | **Owner** |
| **DH:** Legal costs materially exceed annual budget because of unforeseen litigation. | Use of reserves, up to contingency level available.<br>DH kept abreast of current situation and are a final source of additional funding if required. | Monthly – Morounke Akingbola |
| **DH:** GIA funding could be reduced due to changes in Government/policy. | A good relationship with DH Sponsors, who are well informed about our work and our funding model. | Accountability quarterly meetings (on-going) – Richard Sydee |
| | Annual budget agreed with DH Finance team alongside draft business plan submission. GIA funding has been provisionally agreed through to 2020. | December annually – Richard Sydee |
| | Detailed budgets for 2017/18 have been agreed with Directors. DH has previously agreed our resource envelope. | In place – Morounke Akingbola |

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

| **Inherent risk level:** | | | **Residual risk level:** | | |
|---|---|---|---|---|---|
| Likelihood | Impact | Inherent risk | **Likelihood** | **Impact** | **Residual risk** |
| 4 | 4 | 16 – 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. We are currently in a period of turnover and internal churn, with some knowledge gaps, and IfQ related work ongoing until September. Turnover is also variable, and so this risk will be retained on the risk register, and will continue to receive ongoing management attention. |

| Causes / sources | Mitigations | Timescale / owner |
|---|---|---|
| High turnover, sick leave etc., leading to temporary knowledge loss and capability gaps. | Staff have access to Civil Service Learning (CSL); expectation is five working days per year of learning and development for each member of staff.<br>Staff are encouraged to identify personal development opportunities with their manager, through the PDP process, making good use of CSL. | In place – Rachel Hopkins/Peter Thompson |
| | Organisational knowledge captured via documentation, handovers and induction notes, and manager engagement. | In place – Rachel Hopkins |
| | Vacancies are addressed speedily, and any needed changes to ways of working or backfill arrangements receive immediate attention. | In place – Peter Thompson |
| Poor morale leading to decreased effectiveness and performance failures. | Engagement with the issue by managers through team and one-to-one meetings to obtain feedback and identify actions to be taken. | In place – Peter Thompson |

| | | |
|---|---|---|
| | Implementation of staff survey outcomes, followed up after December 2016 staff conference. Task and Finish Groups working on ideas for improvements. | Survey and staff conference done – Rachel Hopkins<br>Follow-up plan and communications in place – Peter Thompson |
| Particular staff changes could lead to specific knowledge loss and low performance. | CMG and managers prioritise work appropriately when workload peaks arise. | In place – Peter Thompson |
| | Policies and processes to treat staff fairly and consistently, particularly in scenarios where people are or could be 'at risk'. | In place – Peter Thompson |
| Insufficient Register team resource to deal properly with OTR enquiries. | Additional member of staff dedicated to handling such enquiries. IfQ delivery means there is still pressure on team capacity. | In place – Nick Jones |
| Increased workload either because work takes longer than expected or reactive diversions arise. | Careful planning and prioritisation of both business plan work and business flow through our Committees. Regular oversight by CMG – standing item on planning and resources. | In place – Paula Robinson |
| | Oversight of projects by both Programme Board and CMG, to ensure that projects end through due process (or closed, if necessary). | In place – Paula Robinson |
| | Learning from Agile methodology to ensure we always have a clear 'definition of done' in place, and that we record when products/outputs have met the 'done' criteria and are deemed complete. | Partially in place – agile approach to be brought into project processes – Paula Robinson |
| | Early emphasis on team-level service delivery planning for the next business year, with active involvement of team members. CMG will continue to review planning and delivery. | |
| | Planning prioritising IfQ/data submission project delivery, and therefore strategy delivery, within our limited resources. | In place until project ends (Autumn 2017) – Paula Robinson |

| | | |
|---|---|---|
| Possible future increase in capacity and capability needed to process mitochondrial donation applications. | Starting to be considered now, but will not be known for sure until later, so no controls can yet be put in place. Only one clinic licensed to provide these treatments, applications are unlikely to be many.<br><br>New licensing processes are in place, ready for first use (decision trees etc.). | Issue for further consideration – Juliet Tizzard |
| Technical issues with our communications systems since our office move in 2016. This leads to poor service (missed calls, poor quality Skype meetings), reputational impacts, additional costs (meetings having to be held externally), and potentially to complaints. | IT team working to identify and resolve the issues, with staff encouraged to continue to send support tickets. External expert commissioned to assist.<br><br>Continued use of external venues with appropriate facilities.<br><br>Use of mailboxes to provide an alternative channel when Skype calls are not received (however there are also some problems with these too). | In progress – Dave Moysen and Nick Jones |
| **Risk interdependencies (ALBs / DH)** | **Control arrangements** | **Owner** |
| **Government/DH:**<br><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><br>We have also been reviewed extensively (including the McCracken review and Triennial Review). | In place – Peter Thompson |

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

| **Inherent risk level:** | | | **Residual risk level:** | | |
|---|---|---|---|---|---|
| Likelihood | Impact | Inherent risk | **Likelihood** | **Impact** | **Residual risk** |
| 4 | 4 | 16 – High | **4** | **3** | **12 - High** |
| **Tolerance threshold:** | | | | | **9 - Medium** |

| **Risk area** | **Risk owner** | **Links to which strategic objectives?** | **Trend** |
|---|---|---|---|
| **Organisational change**<br>OC1: Change-related instability | Peter Thompson, Chief Executive | Whole strategy | ⇧<br>(Added in February 2017) |

| **Commentary** |
|---|
| **Above tolerance.** |

| **Causes / sources** | **Mitigations** | **Timescale / owner** |
|---|---|---|
| The change period may lead to dips in morale, commitment, discretionary effort and goodwill.<br>There are likely to be differential impacts as different changes affect different groups of staff at different times.<br>Risks are to the delivery of current work, including IfQ, and possibly technical or business continuity risks. | Clear published process, with documentation. | In place – Peter Thompson |
| | Consultation, discussion and communication, with opportunity to comment, and being responsive and empathetic about staff concerns. Staff informed of likely developments and next steps and, when applicable, of personal role impacts and choices. | Completed – Peter Thompson |
| | Relatively short timeline for decision making, so that uncertainty does not linger. | In place – Peter Thompson |
| | HR policies and processes are in place to enable us to manage any individual situations that arise. | In place – Rachel Hopkins |
| | Employee assistance programme (EAP) support accessible by all. | In place – Peter Thompson |

| | | |
|---|---|---|
| Organisational change combined with other pressures for particular teams could lead to specific areas of knowledge loss lasting some months (pending recruitment to fill any gaps). | Policies and processes to ensure we treat staff fairly and consistently, particularly those 'at risk'. We will seek to slot staff who are at risk into other roles (suitable alternative employment). | In place – Peter Thompson |
| | Well established recruitment processes, which can be followed quickly in the event of unplanned establishment leavers. | In place – Rachel Hopkins |
| | Good decision-making and risk management mechanisms in place. Knowledge retention via good records management practice, SOPs and documentation. | In place – Peter Thompson |
| Potential impact on our ability to complete IfQ on time. | Ability to use more contract staff if need be. | In place – Peter Thompson |
| Implementing the new structure involves significant additional work across several teams to embed it so that the benefits are realised. There will also be result in some internal churn. | Business plan discussions acknowledging that work in teams doing IfQ or organisational change should not be overloaded. | In place – Paula Robinson |
| | CMG able to change priorities or timescales if necessary, to ensure that change is managed well. | In place – Paula Robinson |
| | Organisational development activity will continue, including summer awayday, to support new ways of working development | In place for coming year – Rachel Hopkins |
| Additional pressure on SMT, HR and Heads, arising from the need to manage different impacts and responses in a sensitive way, while also implementing formal processes and continuing to ensure that work is delivered throughout the change period. | Recognition that change management requires extra attention and work, which can have knock-on effects on other planned work and on capacity overall. Ability to reprioritise other work if necessary. | In place – Peter Thompson |
| | Time being set aside by managers to discuss the changes with staff as needed, with messaging about change repeated via different channels to ensure that communications are received and understood. | In place – Peter Thompson |
| | SMT/CMG additional informal meetings arranged to enable mutual support of managers, to help people retain personal resilience and be better able to support their teams. | In place – Paula Robinson |
| Level of service to Authority members may suffer while the changes are implemented, negatively impacting on the relationship between staff and members. | Communicate the changes clearly to Authority members so that they understand when staff are particularly under pressure, and that they will have reduced capacity. Inform Members when staff are new in post, to understand that those staff need the opportunity to learn and to get up to speed. | To be implemented – Peter Thompson |

| | | |
|---|---|---|
| Once the changes have been implemented, a number of staff will simultaneously be new in post. This carries a higher than normal risk of internal incidents and timeline slippages while people learn and teams adapt. | Ensure a settling in period where staff are inducted and learn, and teams develop new ways of working. Formal training and development provided where required.<br>Knowledge management via records management and documentation. | To be implemented – Peter Thompson |
| Bedding down the new structure will necessarily involve some team building time, developing new processes, staff away days to discuss new ways of working, etc. This will be challenging given small organisational capacity and ongoing delivery of business as usual. | Change management will be prioritised so that bedding down occurs and is effective, and does not take an unduly long time. | To be implemented – Peter Thompson |
| | Continuing programme of leadership development for Heads and SMT. | Being planned – Rachel Hopkins |
| The new model may not achieve the desired benefits, or transition to the new model could take too long, with staff losing faith in the model. | The model will be kept under review following implementation to ensure it yields the intended benefits. | To be implemented – Peter Thompson |
| **Risk interdependencies (ALBs / DH)** | **Control arrangements** | **Owner** |
| - | | |

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

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

| Risk area | Risk owner | Links to which strategic objectives? | Trend |
|---|---|---|---|
| **Cyber security**<br>CS1: Security and infrastructure weaknesses | Nick Jones, Director of Compliance and Information | Whole strategy | New (added in April 2017) |

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

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

| | | |
|---|---|---|
| We could become more dependent on external advice and support, with the risk that we cannot identify or fix problems quickly. | Budget available to commission external support when needed. | In place – Nick Jones |
| Confidentiality breach of Register data. | Staff have annual compulsory security training to guard against accidental loss of data or breaches of confidentiality.<br>Secure working arrangements for Register team, including when working at home. | In place – Peter Thompson |
| Loss of Register or other data by staff or through lack of encryption. | Robust information security arrangements, in line with the Information Governance Toolkit, including a security policy for staff, secure and confidential storage of and limited access to Register information, and stringent data encryption standards. | In place – Dave Moysen |
| Register or other data (electronic or paper) becomes corrupted or lost. | Back-ups and warehouse in place to ensure data cannot be lost.<br>Staff have annual compulsory security training to guard against accidental loss of data or breaches of confidentiality. | In place – Nick Jones/ Dave Moysen |
| Infrastructure turns out to be insecure, or we lose connection and cannot access our data. | IT strategy agreed, including a thorough investigation prior to the move to the Cloud, with security and reliability factors considered. | In place – Dave Moysen |
| | Deliberate internal damage to infrastructure, or data, is controlled for through off-site back-ups and the fact that any malicious tampering would be a criminal act. | In place (March 2015) – Nick Jones |
| Business continuity issue (whether caused by cyber-attack or an event affecting access to Spring Gardens). | Business continuity plan and staff site in place. Regular testing in place, with follow-up.<br>New technology options being explored, to enable us to restore critical on premise systems into a cloud environment if our premises become unavailable for a period.<br>Records management systems to be reviewed in 2017/18. During an outage, staff cannot access TRIM, our current records management system. | In place – Richard Sydee<br>Update done Dave Moysen – September 2016 |
| Poor records management or failure of the document management system. | A comprehensive review of our records management practices and document management system (TRIM) will be conducted in 2017, following planned organisational changes and the conclusion of IfQ. | To follow after organisational re-shaping – Peter Thompson |

| | | |
|---|---|---|
| Cloud-related risks. | Detailed controls set out in 2017 internal audit report on this area.<br><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 – Nick Jones |
| **Risk interdependencies (ALBs / DH)** | **Control arrangements** | **Owner** |
| None.<br><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 | 4 | 20 – Very high | **5** | **3** | **15 - 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** |
|---|
| **Above tolerance.**<br>The judgment on consent to legal parenthood in 2015 and subsequent cases have administrative and policy consequences for the HFEA. Further cases were heard in May 2017. The evidence suggest that we are near the end of these historic cases.<br>A judicial review hearing of one discrete element of the IfQ CaFC project was held in December 2016 and January 2017. The HFEA won this case. A decision by the courts on whether to grant permission to appeal is likely to be heard soon.<br>A licensing matter is currently being challenged and will be considered by the Appeal Committee shortly. If the decision is endorsed we can expect a judicial review. |

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

| | | |
|---|---|---|
| Decisions or our decision-making processes may be contested. Policy changes may also be used as a basis for challenge (Licensing appeals and/or JRs).<br><br>Note: New guide to licensing and inspection rating (effective from go-live of new website) on CaFC may mean that more clinics make representations against licensing decisions. | Legal panel in place, as above. | In place – Peter Thompson |
| | Maintaining, keeping up to date and publishing licensing SOPs, committee decision trees etc. to ensure we take decisions well.<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 2015). | In place – Paula Robinson |
| | Well-evidenced recommendations in inspection reports. | In place – Sharon Fensome-Rimmer |
| Moving to a bolder strategic stance, eg on add ons or value for money, could result in claims that we are adversely affecting some clinics' business model or acting beyond our powers. Any changes could be perceived as a threat – not necessarily ultimately resulting in legal action, but still entailing diversion of effort. | Risks considered whenever a new approach or policy is being developed.<br><br>Business impact target assessments carried out whenever a regulatory change is likely to have a cost consequence for clinics.<br><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><br>Major changes are consulted on widely. | In place – Juliet Tizzard |
| Subjectivity of judgments means we often cannot know which way a ruling will go, and the extent to which costs and other resource demands may result from a case. | Scenario planning is undertaken at the initiation of any likely action. | In place – Peter Thompson |
| Legal proceedings can be lengthy and resource draining. | Panel in place, as above, enabling us to outsource some elements of the work. | In place – Peter Thompson |
| | Internal mechanisms (such as the Corporate Management Group, CMG) in place to reprioritise work should this become necessary. | In place – Peter Thompson |
| Adverse judgments requiring us to alter or intensify our processes, sometimes more than once. | Licensing SOPs, committee decision trees in place. | In place – Paula Robinson |

| | | |
|---|---|---|
| HFEA process failings could create or contribute to legal challenges, or weaken cases that are otherwise sound, or generate additional regulatory sanctions activity (eg, legal parenthood consent). | Licensing SOPs, committee decision trees in place. | In place – Paula Robinson |
| | Up to date compliance and enforcement policy and related procedures. | In place – Nick Jones / Sharon Fensome-Rimmer |
| | Seeking robust assurance from the sector regarding parenthood consent issues, and detailed plan to address identified cases and anomalies. | In progress – Nick Jones |
| **Risk interdependencies (ALBs / DH)** | **Control arrangements** | **Owner** |
| **DH:** HFEA could face unexpected high legal costs or damages which it could not fund. | If this risk was to become an issue then discussion with the Department of Health would need to take place regarding possible cover for any extraordinary costs, since it is not possible for the HFEA to insure itself against such an eventuality, and not reasonable for the HFEA's small budget to include a large legal contingency. This is therefore an accepted, rather than mitigated risk. It is also an interdependent risk because DH would be involved in resolving it. | In place – Peter Thompson |
| **DH:** Legislative interdependency. | Our regular communications channels with the Department would ensure we were aware of any planned change at the earliest stage. Joint working arrangements would then be put in place as needed, depending on the scale of the change. If necessary, this would include agreeing any associated implementation budget.<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 of our regulatory effectiveness being compromised in the event that we are unable to make use of our improved data and intelligence to ensure high quality care.

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

| **Risk area** | **Risk owner** | **Links to which strategic objectives?** | **Trend** |
|---|---|---|---|
| **Regulatory effective-ness**<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 | New (added in May 2017) |

| **Commentary** |
|---|
| **At tolerance.** |

| **Causes / sources** | **Mitigations** | **Timescale / owner** |
|---|---|---|
| IfQ has taken longer than planned, and there will be some ongoing development work needed. | The data submission project is well planned and under way after initial delays.<br>Data cleansing is being done to improve the quality of the data in the Register.<br>The new Register has been designed to be easier to extract data from for analytical purposes. | Completion of data submission project anticipated by August 2017 – Nick Jones |
| Risks associated with data migration to new structure, together with records accuracy and data integrity issues. | IfQ programme groundwork focused on current state of Register. Extensive planning in place, including detailed research and migration strategy. | In place – Nick Jones/Dave Moysen |
| 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. | In place – Nick Jones |

| | | |
|---|---|---|
| Reliability of existing infrastructure systems – (eg, Register, EDI, network, backups). | Maintenance of desktop, network, backups, etc. core part of IT business as usual delivery. | In place – Dave Moysen |
| The new Intelligence team is critical to the new model, and will need to develop an information strategy before it will be possible to use the data for regulatory and other purposes. | Recruitment for a Head is in progress now and will soon be complete. The development of the team, and the information strategy, will follow.<br>The data submission project has been delayed but is now making good progress. | In place – Juliet Tizzard |
| Benefits of IfQ not maximised and internalised into ways of working. | During IfQ delivery, product owners have been in place, and a communications plan. The changes were developed involving the right staff expertise (as well as contractors) and part of the purpose of this was to ensure that the changes are culturally embraced and embedded into new ways of working. | In place (from June 2015) – Nick Jones |
| Insufficient capability and capacity in the Compliance team to enable them to act promptly in response to the additional data that will be available. | Experienced inspection team and business support team, at full complement.<br>An Information Strategy will be produced by the new Intelligence team, to ensure that data analysis and associated internal mechanisms are in place. | In place – Nick Jones<br>To be developed – Head of Intelligence when recruited – Juliet Tizzard |
| Organisational change could take too much time to embed, the necessary culture shift may not be achieved, or new structure not accepted, with an accompanying risk to our ability to make full use of our data and intelligence as intended by the new organisational model. | Organisational re-shaping in progress, to set the right staffing structure and capabilities in place to ensure we can realise IfQ's benefits. This includes the establishment of an Intelligence team. | New organisational model in place – Peter Thompson |
| Regulatory monitoring may be disrupted if Electronic Patient Record System (EPRS) providers are not able to submit data to the new register structure until their software has been updated. | Earlier agreements to extend IfQ delivery help to address this risk by extending the release date for the EDI replacement (IfQ release 2).<br>Mitigation plans for this risk have been agreed as part of planning. | Mitigation in place - Nick Jones |
| Monitoring failure. | Outstanding recommendations from inspection reports are tracked and followed up by the team. | In place – Sharon Fensome-Rimmer |

| | | |
|---|---|---|
| Data accuracy in Register submissions. | Continuous work with clinics on data quality, including verification processes, steps in the OTR process, regular audit alongside inspections, and emphasis on the need for life-long support for donors, donor-conceived people and parents. | In place – Nick Jones |
| | Audit programme to check information provision and accuracy. | In place – Nick Jones |
| | IfQ work has identified data accuracy requirements for different fields as part of migration planning, and will put in place more efficient processes. | In place – Nick Jones |
| | If subsequent work or data submissions reveal an unpreventable earlier inaccuracy (or an error), we explain this transparently to the recipient of the information, so it is clear to them what the position is and why this differs from the earlier provided data. | In place – Nick Jones |
| | Data verification work (February 2017) in preparation for Register migration will improve overall data accuracy, and the exercise includes tailored support for individual clinics that are struggling. | In place – Nick Jones |
| Excessive demand on systems and over-reliance on a few key expert individuals – request overload – leading to errors | PQs, FOIs and OTRs have dedicated expert staff/teams to deal with them.<br>We have systems for checking consistency of answers and the flexibility to push PQ deadlines if necessary. FOI requests are refused when there are grounds for this.<br>PQ SOP revised and log created, to be maintained by Committee and Information Officer/Scientific Policy Manager. | In place – Juliet Tizzard / Paula Robinson |
| Insufficient understanding of our data and/or of the topic or question, leading to misinterpretation or error. | As above – expert staff with the appropriate knowledge and understanding in place. | In place – Juliet Tizzard / Nick Jones |
| Risk that we do not get enough patient feedback to be useful / usable as soft intelligence for use in regulatory and other processes, or to give feedback of value to clinics. | Communications strategy in place, including more patient feedback.<br>Part of the information strategy will focus on making best use of the information gleaned from patients, and converting our mix of soft and hard data into real outcomes and improvements. | In development – Juliet Tizzard |
| **Risk interdependencies (ALBs / DH)** | **Control arrangements** | **Owner** |
| None | - | - |

## ME1: There is a risk that we will not get key messages and information to patients and clinics through our new website, so failing to bring about positive change.

| **Inherent risk level:** | | | **Residual risk level:** | | |
|---|---|---|---|---|---|
| Likelihood | Impact | Inherent risk | **Likelihood** | **Impact** | **Residual risk** |
| 3 | 5 | 15 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 | Juliet Tizzard<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. | New (added May 2017) |

| Commentary |
|---|
| **At tolerance.** |

| Causes / sources | Mitigations | Timescale / owner |
|---|---|---|
| Our ability to provide patient information via the website or CaFC could be compromised by a website failure or failure to launch the new website following GDS assessment. | We have good cyber-security measures to prevent website attacks, and the new content management system is more reliable than the old one.<br>Detailed preparations are well under way for the next gateway review. | In place – Juliet Tizzard |
| Some of our strategy relies on persuading clinics to do things better. This is harder to put across effectively, or to achieve firm outcomes from. | Communications strategy in place, including social media and other channels as well as making full use of our new website. Stakeholder meetings with the sector in place to help us to underline key campaign messages. | In place – Juliet Tizzard |
| Redeveloped website does not meet the needs and expectations of our audience. | User research was done before the website was developed, to properly understand needs and reasons. | In place – Juliet Tizzard |
| Some information will be derived from data, so depends on risk above being controlled. | See controls listed in RE1, above. | |

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

# Reviews and revisions

### AGC – March 2017 meeting

AGC commented on the 2014-2017 strategic risk register, and noted that the new version would come to the next meeting. AGC particularly noted the ongoing unpredictability of our PQ and FOI requests, and their complexity.

### CMG – May 2017 meeting

CMG reviewed the new risk register and made the following points in discussion:
The new risk register comprised two types of strategic risk: generic high level risks to the infrastructure and general operation of the HFEA, affecting the whole strategy, and specific risks to elements of the strategy. The generic risks are financial viability, people-related risks, cyber-security and legal risks.

CMG discussed whether to combine the two people-related risks areas of 'Capability' and 'Change'. Although the organisational changes have now been agreed, resulting in some overlap, CMG agreed it was appropriate to retain the separate organisational change risk for a few months, while the new organisational structure is fully implemented.

CMG agreed that beyond the generic category of risk, there were two main risks to delivery of the strategy:

- Regulatory effectiveness – if we are unable to make use of our improved data and intelligence to ensure high quality care, for example through our aim to do more targeted regulatory interventions.
- Messaging, engagement and information provision – if we were unable to use our new website and other channels effectively to convey and promote key messages and information to patients and clinics, for example about treatment add ons or improved support.

CMG agreed that the products of IfQ should now be listed among the controls for these risks, rather than retaining IfQ as a separate risk area. We continue to manage the remaining IfQ delivery risks through the IfQ Programme Board and the IfQ risk log, and will continue to report regularly to AGC and the Authority on risks and progress, until the work has been completed.

# 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 | | | | |

## 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

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

# 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 | 15 | | |
| Paper number | AGC (13/06/2017) 555 | | |
| Meeting date | 13 June 2017 | | |
| Author | Morounke Akingbola, Head of Finance | | |
| **Output:** | | | |
| For information or decision? | Decision | | |
| Recommendation | The Committee is asked to review and make any further suggestions and comments and agree the plan. | | |
| Resource implications | None | | |
| Implementation date | N/A | | |
| Organisational risk | ☒ Low | ☐ Medium | ☐ High |
| | Not to have a plan risks incomplete assurance, inadequate coverage or unavailability key officers or information | | |
| Annexes | N/A | | |

# Audit & Governance Committee Forward Plan

| AGC Items Date: | 21 Mar 2017 | 13 Jun 2017 | 3 Oct 2017 | 5 Dec 2017 |
|---|---|---|---|---|
| Following Authority Date: | 10 May 2017 | 28 Jun 2017 | 15 Nov 2017 | Jan 2018 |
| **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<br>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: | 21 Mar 2017 | 13 Jun 2017 | 3 Oct 2017 | 5 Dec 2017 |
|---|---|---|---|---|
| HR, People Planning & Processes | | Yes | | |
| Strategy & Corporate Affairs management | | | Yes | |
| Regulatory & Register management | | | | Yes |
| Resilience & Business Continuity Management | Yes | Yes | Yes | Yes |
| Finance and Resources management | Yes | | | |
| Reserves policy | | | Yes | |
| Review of AGC activities & effectiveness, terms of reference | | | | Yes |
| Legal Risks | | | Yes | |
| AGC Forward Plan | Yes | Yes | Yes | Yes |
| Session for Members and auditors | Yes | Yes | Yes | Yes |
| Other one-off items | | | | |