

Audit and Governance Committee meeting - agenda

7 December 2016

River Meeting Room

King's College London, Strand Campus, Strand, London WC2R 2LS

Agenda item	Time
1. Welcome, apologies and declaration of interests	10:00am
2. Minutes of 21 September 2016 [AGC (07/12/2016) 512]	
3. Matters Arising [AGC (07/12/2016) 513 MA]	
4. Rating [Oral - Jon Whitfield, Government Internal Audit Agency (GIAA)]	
5. Register & Compliance Risks [Presentation NJ]	
6. Information for Quality (IfQ) Programme – Managing Risks [AGC (07/12/2016) 514 NJ]	
7. Strategic Risks [AGC (07/12/2016) 515 PR]	
8. Internal Audit a) Progress report 2016/17 [AGC (07/12/2016) 516 DH Internal Audit]	
9. External Audit a) Audit Planning Report [AGC (07/12/2016) 517 NAO]	
10. Implementation of Recommendations – Progress Report [AGC (07/12/2016) 518 WEC]	

11.	Cyber Security - Information Security & Testing [AGC (07/12/2016) 519 DM]	
12.	Disclosure and Barring Service (DBS) checks [Oral RH]	
13.	Resilience & Business Continuity Management [Oral DM]	
14.	Whistle Blowing Policy [AGC (07/12/2016) 520 MA]	
15.	Contracts & Procurement [Oral MA]	
16.	Review of AGC activities & effectiveness [AGC (07/12/2016) 521 SK]	
17.	AGC Forward Plan [AGC (07/12/2016) 522 MA]	
18.	Any other business	
19.	Close (Refreshments & Lunch provided)	1.15pm
20.	Session for members and auditors only	1.15pm
21.	Next Meeting	10am Tuesday, 21 March 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 (07/12/2016) 512
Meeting date	7 December 2016
Author	Dee Knoyle, 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	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High

Annexes

Minutes of Audit and Governance Committee meeting held on 21 September 2016 at HFEA, 10 Spring Gardens, London SW1A 2BU

Members present Rebekah Dundas (Chair)
 Gill Laver
 Jerry Page
 Anita Bharucha

Apologies Margaret Gilmore

External advisers Internal Audit:
 Paul Foreman, Price Waterhouse Coopers (PWC)

 National Audit Office (NAO):
 Sarah Edwards

Observers Kim Hayes (Department of Health)

Staff in attendance Peter Thompson, Chief Executive
 Morounke Akingbola, Head of Finance
 Adam Ashiwaju, Accounts Officer
 Juliet Tizzard, Director of Strategy and Corporate Affairs
 Nick Jones, Director of Compliance and Information
 David Moysen, Head of IT
 Paula Robinson, Head of Business Planning
 Ian Brown, Head of Corporate Governance
 Dee Knoyle, Committee Secretary

1. Welcome, apologies and declarations of interests

1.1 The Chair welcomed attendees to the meeting.

1.2 There was one apology from Margaret Gilmore.

1.3 The Chair made the following announcements:

- Sally Cheshire, Chair of the Authority will continue the role for a further three years.
- Margaret Gilmore will become Deputy Chair of the Authority from November 2016.

Margaret will remain a member of the Audit and Governance Committee until the end of December 2016 and will continue her role on the Licence Committee. Margaret will also take on the role of Chair of the Statutory Approvals Committee from October 2016.

- Rebekah Dundas will be leaving the Authority in December 2016 as her term has come to an end.
- Anita Bharucha will become Chair of the Audit and Governance Committee from January 2017.
- Sue Gallone will be retiring from the HFEA in September 2016. Members acknowledged her hard work and expressed sincere and grateful thanks for her support.

- Richard Sydee has been appointed Director of Finance and Resources and will start this role on 1 November 2016.
- Ian Brown, Head of Corporate Governance will be leaving the HFEA on 30 September 2016 and interim arrangements will be in place until recruitment begins for this role.

1.4 There were no declarations of interest.

2. Minutes of the meeting held on 16 March 2016

2.1 The minutes of the meeting held on 15 June 2015 were agreed as a true record of the meeting and approved for signature by the Chair.

3. Matters arising

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

3.2 e) The two external members of the committee, Gill Laver and Jerry Page are awaiting suitable dates to attend an Authority meeting as an observer.

3.3 9.6) The Information Governance Group are establishing a meeting date.

3.4 12.6) The Executive will review the Appeals process and consider what a proportionate first step, the representations would look like. Work will start in October 2016 and recommendations will be presented to the Authority by the end of the business year.

3.5 14.5) The Triennial review report is expected to be circulated to Arm's Length Bodies (ALBs) shortly after political party conferences which take place in October.

3.6 5.7) The Information for Quality (IfQ) Internal Systems Project Manager will circulate a list of recommendations and planned actions (relating to 'Public Beta') to the committee after review by Programme Board.

3.7 8.5) The Executive is consulting with other healthcare professionals on Disclosure and Barring Service (DBS) checks and will take a light touch approach. The Executive will aim to feed back to the Audit and Governance committee at the meeting in December 2016.

4. Strategy and Corporate Affairs Management

4.1 The Director of Strategy and Corporate Affairs provided the committee with a presentation and briefing on managing the Directorate's risks tied to the corporate strategy, the current risks over the next 6 months.

4.2 The committee was reminded of the content of the update on the Directorate presented last year.

4.3 The committee noted the Directorate's contributions to the HFEA Strategy which focuses on setting standards, increasing and informing choice and efficiency, economy and value. The focus of the Strategy has shifted from regulatory in previous years to patients' needs.

4.4 Understanding patients' needs at all stages of treatment has shaped the design of services such as Choose a Fertility Clinic on the new HFEA website, where the brand has been refreshed and the tone of voice has changed. New features on the website include a donor egg and sperm availability service and a new patient rating service, allowing patients to review a clinic's performance before treatment.

- 4.5** A new counselling and support service for people seeking donor information or re-registering has also been launched.
- 4.6** The HFEA has continued to inform patient choice by publishing reports such as fertility trends and sharing information on new or tested treatments.
- 4.7** The Executive has established a working relationship with NHS (National Health Service) Choices and plan to apply for Information Standards, awarded by NHS (National Health Service) England for good quality patient information.

Key Risks:

- 4.8** Patient: The committee noted that further work is required to market the services provided by the HFEA as a regulator, to ensure that information is accessed at the appropriate time, especially at the early stages when a patient is first seeking treatment.
- 4.9** Stakeholder engagement: The committee noted that there has been a legal challenge to the presentation of clinic information on Choose a Fertility Clinic on the new HFEA website. The Executive is engaging with the sector and seeking acceptance from all clinics to ensure that the planned services are fully delivered.
- 4.10** Communication: The new website is due to become live in January/February 2017. However, the content management system on the existing website is dated and no longer supported by the original supplier which has led to instability from time to time. The committee was informed that should the HFEA website fail to operate completely for a period of time, other forms of communication would be used to communicate with stakeholders and the public via the HFEA Portal and social media. Due to recent delays to the programme, the committee advised the Executive to consider seeking support for the content management system of the existing website in the interim, until the new website is available, as the risk of the existing website failing will increase with time. The committee noted that there are financial costs involved and agreed that this should be an option.

Action

- 4.11** Head of Communications to seek support for the content management system for the existing website in the interim until the new website is available.

5. Information for Quality (IfQ)

- 5.1** The Director of Compliance and Information provided the committee with a paper, presentation and briefing on the delivery of the 'Public Beta' phase of the new Website and Clinic Portal and the plans for data mitigation to the new Register.

5.2 The Programme

The Plan

- 5.3** The committee was informed that following an unexpected legal injunction, relating to the display of clinic information, brought by a clinic in July 2016, which has since been lifted, a judicial review has been scheduled in December 2016 and therefore the delivery plan has been revised, including the next Government Digital Service (GDS) assessment.
- 5.4** The consequences of the updated timeline as well as the judicial review have been assessed and the risks are currently being mitigated.

- 5.5** There has been no formal revision to the budget. However, the Executive is currently working through the consequences of the revised timeline.

Release One - HFEA Website and Clinic Portal

- 5.6** The Programme is now running through its 'Public Beta' phase for both the new Website and Clinic Portal. During this stage, all feedback from the public and stakeholders will be analysed and reviewed for further developments and this process will continue when the system goes live, to ensure that the users' needs are met.

- 5.7** The Government Digital Service (GDS) assessment of the Clinic Portal to enable progression to 'live' is scheduled for October 2016.

- 5.8** The GDS assessment to enable the website to 'go live' has been pushed back to January 2017 due to the pending judicial review.

Release Two – Electronic Data Interchange (EDI) and Electronic Patient Record System (EPRS)

- 5.9** The next phase 'Release two' has completed its planning stage and partially started its development. EDI is now scheduled for February 2017 and EPRS is still on schedule for March 2017.

- 5.10** The Executive is engaging with EPRS providers (suppliers of patient reporting systems to approximately half of all clinics). The providers have been notified of the development path to March 2017 and are well informed, however some providers are not keen to develop systems and there is a risk that some clinics may want to continue using a system which is not aligned to submit data to the HFEA. The Executive plan to maintain a close level of engagement with providers to enable gradual adoption of ways to 'connect' to the HFEA and maintain the necessary security.

- 5.11** The Standardisation Committee for Care Information (part of NHS (National Health Service) Digital) accreditation process for the 'UK ART (Assisted Reproductive Technology) dataset' and its implementation is on schedule.

- 5.12** The overall risk score for the IfQ Programme has increased. The main risk added relates to EPRS providers and the impact on treatment fees linked to the submission of data should there be any delays.

- 5.13** There were three new inter-related strategic risk sources arising from the IfQ programme which would only apply following IfQ Release Two in 2017. These risks included the various impacts if EPRS providers did not make the necessary changes to their systems to submit clinic treatment data to the new Register structure. There would be a risk of loss of regulatory authority as any gaps in data could impact effective regulatory monitoring; a risk to improved information access since any data that had not been provided would not be available to provide to patients through Choose a Fertility Clinic; and also a risk to financial viability – negative impact on cash flow, if the HFEA were not able to bill clinics for treatments provided but not reported. The Executive is currently working to develop further mitigation plans for these risks, alongside the HFEA finance and compliance departments.

Register - Data Migration

- 5.14** The committee was informed that data cleansing and migration work is slightly behind schedule.

- 5.15** Clinics are encouraged to deal swiftly with HFEA requests to fix errors and this process will be monitored closely.

- 5.16** An expert in data migration has been commissioned to provide assurances for all steps leading up to the transfer of data.
- 5.17** The committee noted the legal situation and the impact on the timeline and that this may have financial consequences affecting the budget for the programme. The committee agreed that a report should be provided on the financial consequences as soon as possible.
- 5.18** The committee noted that stakeholder engagement is key to the success of the programme and encouraged the Executive to maintain the momentum.
- 5.19** The committee also asked the Executive to give more consideration to 'plan B' for the website, in the event of an adverse JR judgment, or in the event of Red Dot (the current, outgoing content management system, which was old and unsupported) failing completely.

Action

- 5.20** Director of Compliance and Information to provide a report on the financial consequences as a result of movement to the timeline due to the judicial review as soon as possible.
- 5.21** The Executive to consider mitigations for the website in the event of an adverse JR decision or a complete failure of the current content management system.

6. Strategic Risks

- 6.1** The Head of Business Planning presented the strategic risk register.
- 6.2** The committee discussed the strategic risks, in particular the three risks above tolerance which include improved information access (currently under development in the Information for Quality (IfQ) programme), the risk of incorrect data being released and knowledge and capacity.
- 6.3** The committee was informed that work was underway to develop further mitigation plans for the three new inter-related strategic risk sources arising from the IfQ programme (as discussed at item 5) which would only apply following IfQ Release Two in 2017.
- 6.4** Parliamentary questions fluctuate and there are times when the volumes are challenging to process with a quick turnaround. The committee noted that the Executive is working to capacity and currently doing all that is possible to mitigate the risks of incorrect data released and the standard operating procedures have been revised. The committee noted that the Executive is granted the maximum time to provide answers to Parliamentary questions and this must be adhered to. However, the Department of Health will continue to give early warning to ALBs when there is a rise in the number of Parliamentary questions to be answered.
- 6.5** The committee discussed the new finance risk of non-payment to suppliers, caused by technical issues with migration to internet banking. This has been escalated with the bank and the HFEA finance team are currently working around the situation until the issues have been resolved.
- 6.6** The committee noted the risk relating to knowledge and capacity and was reassured that the risk would not increase as a result of having one vacancy for a member of staff at Head's level.
- 6.7** The Executive has encouraged junior members of staff to learn more about risks to improve awareness and reporting within the organisation.
- 6.8** The committee noted that the Department of Health's risk audit recommendation that Arm's Length Bodies (ALBs) and the Department consider risk interdependencies across the health and care system and the HFEA will seek to embed this approach into future management of risk.

- 6.9** The committee was satisfied with the current controls and mitigation plans in place to manage the organisation's strategic risks.

7. Internal Audit

a) Progress Report

- 7.1** The committee was provided with a progress report on the annual programme.
- 7.2** The audit on income generation has been completed.
- 7.3** The Board effectiveness review is in progress.
- 7.4** The field work on Cyber Risks will begin in November 2016
- 7.5** All field work is to be completed by the end of March 2017.

b) Income Generation

- 7.6** The committee was provided with an Income Generation Report.
- 7.7** The business process was mapped from data submitted by the clinic to the production of invoices and controls were reviewed and tested.
- 7.8** The auditors reported that a few areas in the process could be enhanced including closer monitoring of clinics not submitting data.
- 7.9** The committee questioned why the Executive had resisted some of the recommendations which were low priority. The Executive reassured the committee that the organisation had other means of covering the recommendations which were aligned to the function and capacity of the organisation. The committee acknowledged that the Executive's way of working did not undermine the organisation's control systems, however encouraged the Executive to implement the recommendation relating to data extracted from Sage, accounting software if at all possible.
- 7.10** Risk management controls are to be in place for the new portal before it becomes live. The Management team are confident that they know how to manage the risks using the new software.
- 7.11** The overall rating for income generation was moderate.
- 7.12** The committee discussed the rating system and agreed that Jon Whitfield from the Government Internal Audit Agency (GIAA) will be invited to attend the Audit and Governance Committee meeting in December 2016 to engage in a further discussion on rating.

Action

- 7.13** Jerry Page to invite Jon Whitfield from the Government Internal Audit Agency (GIAA) to attend the Audit and Governance Committee meeting in December 2016 to engage in a further discussion on rating.

8. External audit

- 8.1** The National Audit Office (NAO) provided the committee with an oral update.

- 8.2** The committee noted that an audit planning meeting took place with the HFEA and the NAO on 14 September 2016 and a report will be presented to the Audit and Governance Committee at the meeting in December 2016.
- 8.3** The committee was informed that Sarah Edwards and George Smiles will remain NAO representatives for the HFEA, however the lead auditor has changed from Melini to Payal who has good experience working with smaller Arm's Length Bodies (ALBs).

9. Implementations of recommendations progress report

- 9.1** The Head of Finance provided the committee with an update.
- 9.2** The committee noted that there are currently no outstanding recommendations.

10. Cyber Security

- 10.1** The Head of IT provided the committee with an oral update on the security and testing of the organisation's IT systems.
- 10.2** The new HFEA Portal and website have been tested. There were seven low risk issues which have been resolved.
- 10.3** The design for the architecture for Release Two of the IfQ programme, Electronic Patient Record System (EPRS) has just been completed with the assistance of external experts. Class consultants will complete a review of the infrastructure before moving onto the next steps, creating and testing the system. The committee agreed that the Executive should ask all external expert consultants to provide documented evidence of advice given.
- 10.4** The committee was informed that the review of Release Two by Class consultants would take 4-6 weeks.
- 10.5** Wider testing for the whole organisation will be completed after the testing period for Release Two is complete.
- 10.6** The organisation will be moving to a secure system using the Cloud in future and this will increase security.
- 10.7** A detailed Risk Management and Accreditation Document Set (RMADS), which explains the threats and mitigation will be created and signed off by the SIRO (Senior Information Risk Officer).
- 10.8** The committee highlighted that the legislation requires HFEA data to be fully protected and requested evidence from external providers that they are doing what was agreed and that we have written assurances. The committee agreed that the Head of IT should provide a further update paper on information security and testing at the next meeting in December 2016 including evidence of assurance received.

Action

- 10.9** Head of IT to provide the Audit and Governance Committee with a further update paper on information security and testing and documented evidence of assurances obtained at the next meeting in December 2016.

11. Reserves Policy

- 11.1** The Head of Finance presented the revised Reserves Policy and briefed the committee on the recent changes.
- 11.2** There were revisions to the figures included in the policy but no changes to the actual policy. Key changes included:
- an increase in rent charges due to relocating to the office of NICE (The National Institute for Health and Care Excellence)
 - salary costs – increased slightly
 - The Head of Finance advised the committee that further work on forecasting our income which would impact on reserves will be carried out at a later date.
- 11.3** The committee acknowledged that HFEA income and expenditure may fluctuate in some areas and this is unpredictable for example treatment income and legal costs.
- 11.4** The committee noted that the sum allocated for reserves remains largely the same.
- 11.5** The committee noted the changes and approved the Reserves Policy.

12. Forward plan

- 12.1** The committee was satisfied with the content of the Forward Plan of agenda items for the forthcoming meetings, with the addition of Cyber Security and Internal Audit Ratings to the next agenda in December 2016. The committee also noted that all internal audit work needs to be complete by March 2017 as there is likely to be new suppliers of internal audit.

13. Any other business

- 13.1** There was nothing to report on whistleblowing or suspected fraud incidents and no contracts were awarded since the last meeting.
- 13.2** The Chair thanked attendees for their contributions to the meeting.
- 13.3** Members and auditors retired for their confidential session.
- 13.4** The next meeting will be held on Wednesday, 7 December 2016 at 10am.

Chair's signature

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

Signature

Name

Rebekah Dundas

Date

7 December 2016

Audit and Governance Committee Paper

Paper Title:	Matters arising from previous AGC meetings
Paper Number:	[AGC (07/12/2016) 513 MA]
Meeting Date:	7 December 2016
Agenda Item:	3
Author:	Morounke Akingbola, Head of Finance
For information or decision?	Information
Recommendation to the Committee:	To note and comment on the updates shown for each item.
Evaluation	To be updated and reviewed at each AGC.

Numerically:

- 5 items added from September 2016 meeting, 3 ongoing
- 8 items carried over from earlier meetings, 5 ongoing
- 1 items carried over from AGC self-assessment of performance 2014, 1 ongoing

Matters Arising from Audit and Governance Committee review of performance December 2014			
ACTION	RESPONSIBILITY	DUE DATE	PROGRESS TO DATE
e) Arrange for external members to attend Authority meeting as observers	Head of Governance & Licensing	September 2015	Ongoing – members invited to meetings, suitable dates to be agreed.
Matters Arising from Audit and Governance Committee – actions from 10 June 2015 meeting			
ACTION	RESPONSIBILITY	DUE DATE	PROGRESS TO DATE
9.6 Report progress on actions from the information governance group to AGC	Director of Finance and Resources	December 2016	Ongoing – Group to establish first meeting.
Matters Arising from Audit and Governance Committee – actions from 9 December 2015 meeting			
ACTION	RESPONSIBILITY	DUE DATE	PROGRESS TO DATE
12.6 The Executive to add a review of the procedures for representations to the Business Plan for 2016/17 and report back to the Authority with recommendations, in due course.	Head of Business Planning	April 2016	Ongoing – added to business plan, work to start in October 2016 and recommendations will be presented to the Authority by the end of the business year.
14.5 The Triennial review report is to be sent to committee members.	Director of Finance	When published	Ongoing – an update is on its way.
Matters Arising from Audit and Governance Committee – actions from 15 June 2016 meeting			
5.7 Circulate a list of recommendations and planned actions (relating to public beta) to the committee after review by Programme Board	Information for Quality (IfQ) Internal Systems Project Manager	January 2017	Ongoing

8.5 Consider the need for possible Security checks for new staff, such as DBS	CEO/Head of HR	October 2016	Completed – Agenda item for December 2016
Matters Arising from Audit and Governance Committee – actions from 21 September 2016 meeting			
4.11 Head of Communications to seek support for the content management system for the existing website in the interim until the new website is available.	Head of Communications	asap	Ongoing
5.20 Director of Compliance and Information to provide a report on the financial consequences as a result of movement to the timeline due to the judicial review as soon as possible.	Director of Compliance & Information	asap	Ongoing
5.21 The Executive to consider mitigations for the website in the event of an adverse JR decision or a complete failure of the current content management system.	Head of Communications	asap	Ongoing
7.13 Jerry Page to invite Jon Whitfield from the Government Internal Audit Agency (GIAA) to attend the Audit and Governance Committee meeting in December 2016 to engage in a further discussion on rating.	Jerry Page, AGC Member	December 2016	Completed – Agenda item for December 2016
10.9 Head of IT to provide the Audit and Governance Committee with a further update paper on information security and testing and documented evidence of assurances obtained at the next meeting in December 2016.	Head of IT	December 2016	Completed – Agenda item for December 2016

Information for Quality (IfQ) Programme – Managing Risks

Strategic delivery:

Setting standards

Increasing and
informing choice

Demonstrating efficiency
economy and value

Details:

Meeting

AGC

Agenda item

5

Paper number

AGC (07/12/2016) 514 NJ

Meeting date

07 December 2016

Author

Nick Jones, Director of Compliance & 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

Annex A –

1. Introduction and summary

- 1.1.** The purpose of this report is to provide the Committee with a progress report on the IfQ Programme. The Programme is currently in the closing stages of its 'public beta' phase for both the new Website and Clinic Portal. Slow but steady progress is being made against Release 2 of the Clinic Portal, which centres on the data submission facility for clinics and the new Register.

2. IfQ projects update

2.1. IfQ Release 1

- The HFEA website work is currently focused on closing the Beta phase, having delivered the key outputs for the project, with some lower priority work remaining before Beta concludes. Valuable user feedback has been collected; there has been substantial stakeholder engagement; and further user research sessions have been completed.
- Further to the outcomes of the November 2016 Authority meeting and pending the judicial review hearing scheduled in December, some further adjustments will be made between now and January 2016 - essentially to the way data is presented on the Website. After this point, the service will undergo a GDS assessment for its readiness to be transitioned to full 'live' service.
- We are now formally verifying with clinics, the data that will be made available on the new Choose a Fertility Clinic facility. Clinics have 12 weeks to verify their data, which is slightly longer than is usual accounting for a slight increase in complexity of the data. This work is expected to conclude in February 2017.
- Release 1 of the Clinic Portal has now also delivered all key outputs of the project, spent considerable time in 'public beta', received its DH/GDS assessment on the 21 November 2016, and on 28 November 2016 a full pass assessment was received. The team is now preparing to go live, and preparing to de-commission the existing Clinic Portal. There is a few weeks' work to do this. This is obviously extremely gratifying for the team.

2.2. IfQ release 2

- This relates to the treatment data submission system, much awaited by clinics. It is 'Release 2' because it forms part of the Clinic Portal (Release 1). Release 2 of the Clinic Portal has been making slow but steady progress. This builds on the substantial amount of foundational work that the HFEA has completed over the last year to prepare for the development of Release 2, including the finalisation of the new Register structure, data cleansing, and internal systems infrastructure completed during Release 1.

- Despite good progress, the work has slowed due to a continued focus on finalising Release 1 at a time when the teams were anticipated to be working solely on Release 2. As a result, the risk of not delivering the required outputs in line with the current budget constraints and within this financial year have grown sharply. In response, the Programme team has conducted an exercise to re-examine programme scope and the management and support structure in order to reduce this risk. It is evident that without a further addition of resources, Release 2 of the Clinic Portal will not be substantially complete until end of Q1 2017. (See annex A)
- Having explored the scope, and rescheduled, a further option is to explore securing additional resources to bring the completion date forward. The Programme has been run very tightly in terms of resources and has absorbed several unexpected events over its course (albeit these are inevitable in almost any programme). Further, the team is aware that the fate of many IT-based transformation programmes is cost and time overruns.
- The team has focused on the costs of continued involvement of key programme resource at an estimated cost of an additional up to £90k. We continue to review the merits of this approach, and the scope for permitting this within the rules, with DH. This additional budget is expected to enhance the likelihood that all key deliverables of Release 2 are complete by April 2017.
- The Standardisation Committee for Care Information (part of NHS Digital) accreditation process for the 'UK ART dataset' and its implementation has been delayed to March 2017 accommodate dependencies with development activity that is now anticipated to take place in early 2017.

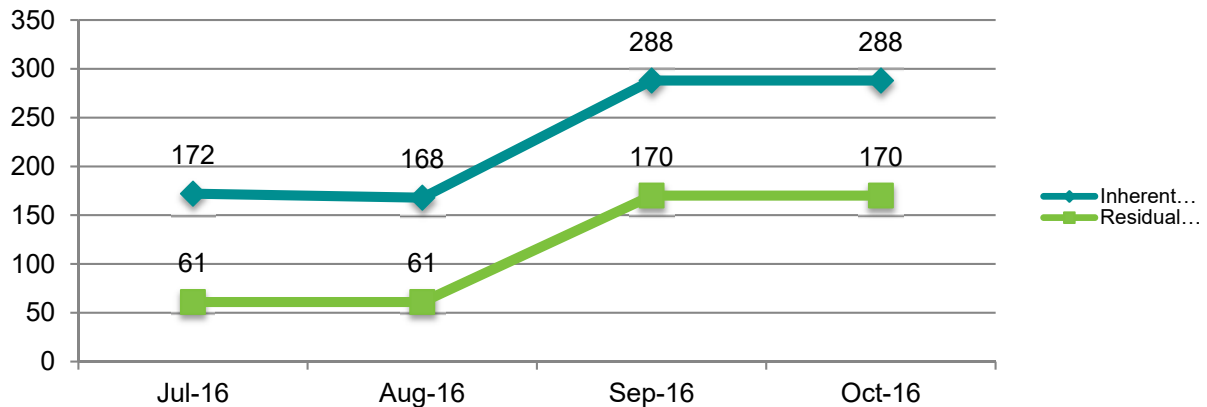
2.3. IfQ data cleansing/Migration

- Data cleansing work has now dealt with all 'severity 1' items that are possible to address. This is an important milestone for the IfQ Programme, as these issues would have prevented the 'data migration' process from progressing.
- Due to the continued diversion of key resource to Release 1, the data migration of the existing (cleansed) database to a new structure is behind schedule. Trial Load 1 has been run, with the team working towards running Trial Load 2 in December 2016. Assurance services for the data migration are now anticipated to provide their first assurance audit in January 2017. Data Migration is now anticipated to be finally completed in April 2017.

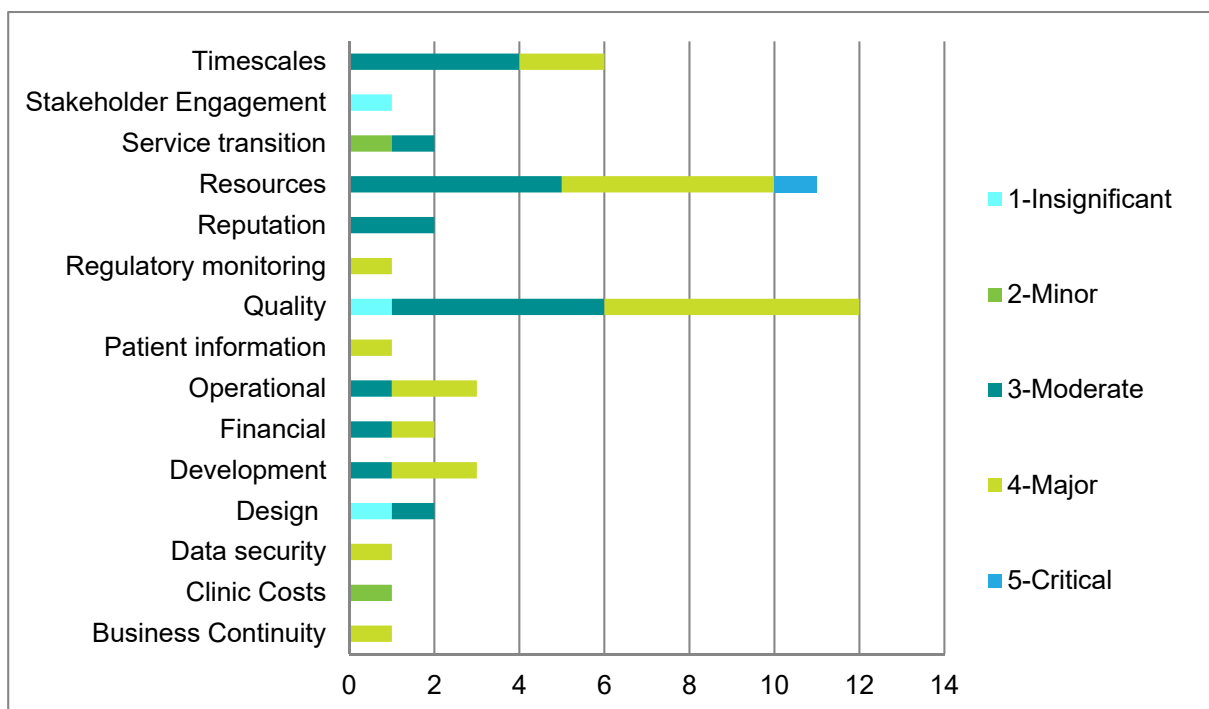
3. IfQ risks and issues

3.1. Overall update

- The line graph below represents the overall IfQ risk score, which combines the perceived impact and likelihood of the current risks on hand each month.
- The overall risk score for the IfQ Programme has significantly increased in the last month, all risks have been reviewed mitigated and escalated to SMT as per the governance processes in place and are currently being monitored.



- The major risks are associated with resources, timescales, regulatory monitoring, quality, financial, development, patient information, data security and business continuity.



4. IfQ budget

4.1. The current budget position (excluding VAT) for 2016/17 is as follows:

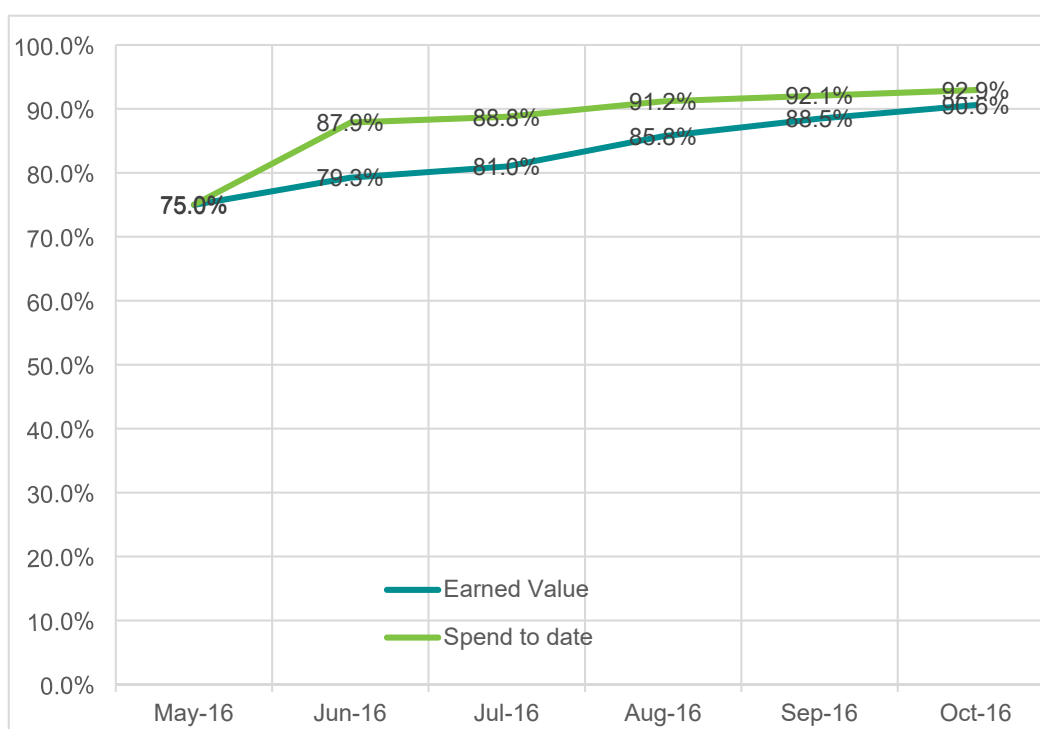
Total IfQ budget May 2016	Budget this F/Y (16/17)	Planned spend (Oct 2016)	Actual to date (Oct 2016)	Monthly Variance
1,227,402	£619,025	£1,171,626	£1,158,700	£12,926

4.2. The delay to the programme had some financial consequences, the detailed of the proposed plan is explained above.

5. Earned value

- The spend to date has raised slightly comparing to last month and is now again joining the earned value. As we reach the end of beta and complete the live phase we expect the earned value to reach its peak reflecting the work completed.

Period	May-16	Jun-16	Jul-16	Aug-16	Sep-16	Oct-16
Earned Value	75%	79%	81%	85.8%	88.5%	90.6%
Spend to date	75%	87%	88%	91.2%	92.1%	92.9%



6. Recommendation:

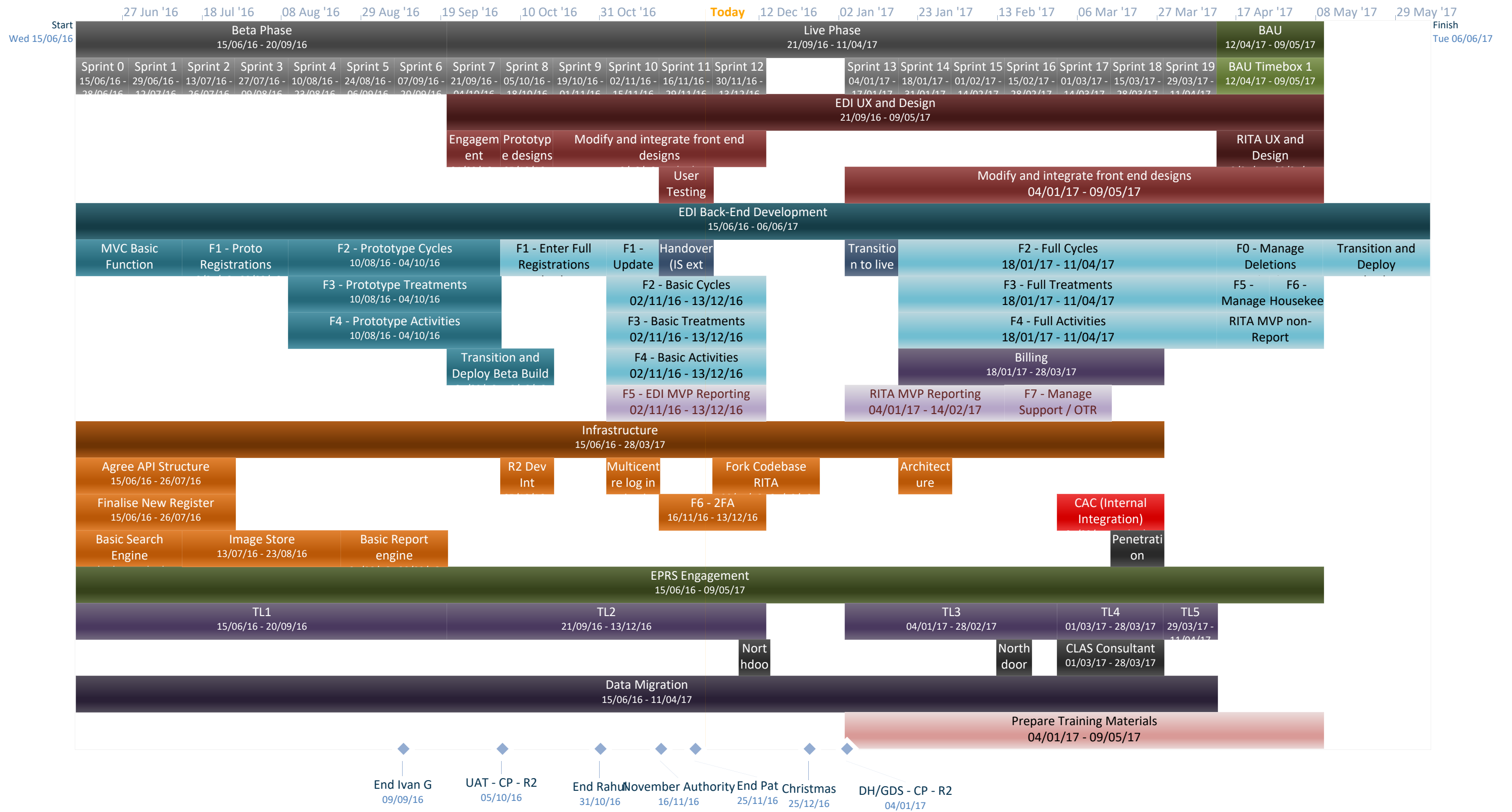
6.1. The Audit and Governance Committee is asked to:

- Note progress, risks and the budget position on IfQ.
- Note in particular the update on the new risks.

7. Annexes:

- Annex A: Timeline for the remaining IfQ Beta phase

Attachment – Proposed Release Plan for IfQ Release 2 Sprints



Strategic risks

Strategic delivery:	<input checked="" type="checkbox"/> Setting standards	<input checked="" type="checkbox"/> Increasing and informing choice	<input checked="" type="checkbox"/> Demonstrating efficiency economy and value
Details:			
Meeting	Audit and Governance Committee		
Agenda item	7		
Paper number	[AGC (07/12/2016) 515 PR]		
Meeting date	7 December 2016		
Author	Paula Robinson, Head of Business Planning		
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. CMG reviews risk quarterly in advance of each AGC meeting. AGC reviews the strategic risk register at every meeting. The Authority reviews the strategic risk register periodically.		
Organisational risk	<input type="checkbox"/> Low	<input checked="" type="checkbox"/> Medium	<input type="checkbox"/> High
Annexes	Annex 1: Strategic risk register		

1. Strategic risk register

Latest reviews

- 1.1. The Authority noted the risk register at its meeting on 16 November. CMG reviewed the risk register on 23 November 2016. CMG discussed all risks, their controls, and scores. Three of the twelve risks are currently above tolerance.
- 1.2. The current strategic risk register is attached at Annex A, and includes an overview of CMG's recent discussions about the risk register. The annex includes the graphical overview of residual risks plotted against risk tolerances.

2. Recommendation

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

HFEA strategic risk register 2016/17

Annex A

Risk summary: high to low residual risks

Risk area	Risk title	Strategic linkage ¹	Residual risk	Current status	Trend*
Information for Quality	IfQ3: Delivery of promised efficiencies	Efficiency, economy and value	12 – High	Above tolerance	↔↓↔↑
Data	D2: Incorrect data released	Efficiency, economy and value	12 – High	Above tolerance	↔↔↔↑
Capability	C1: Knowledge and capability	Efficiency, economy and value	12 – High	Above tolerance	↔↔↔↑
Legal challenge	LC1: Resource diversion	Efficiency, economy and value	12 – High	At tolerance	↔↔↔↔
Data	D1: Data loss or breach	Efficiency, economy and value	10 – Medium	At tolerance	↔↔↔↔
Financial viability	FV1: Income and expenditure	Efficiency, economy and value	9 – Medium	At tolerance	↔↔↔↔
Donor conception	DC2: Support for OTR applicants	Setting standards: donor conception	9 – Medium	At tolerance	↔↔↔↔
Regulatory model	RM1: Quality and safety of care	Setting standards: quality and safety	8 – Medium	At tolerance	↔↔↔↔
Regulatory model	RM2: Loss of regulatory authority	Setting standards: quality and safety	8 – Medium	At tolerance	↔↔↔↔
Information for Quality	IfQ1: Improved information access	Increasing and informing choice: information	8 – Medium	At tolerance	↔↔↔↓
Information for Quality	IfQ2: Register data	Increasing and informing choice: Register data	8 – Medium	At tolerance	↔↔↔↔
Donor conception	DC1: OTR inaccuracy	Setting standards: donor conception	4 – Low	At tolerance	↔↔↔↔

* This column tracks the four most recent reviews by AGC, CMG, or the Authority (eg, ↑↔↓↔↔).

Recent review points are: Authority 6 July ⇒ CMG 7 September/AGC 21 September ⇒ Authority 16 November (noted) ⇒ CMG 23 November

¹ Strategic objectives 2014-2017:

Setting standards: improving the quality and safety of care through our regulatory activities. (Setting standards – quality and safety)

Setting standards: improving the lifelong experience for donors, donor-conceived people, patients using donor conception, and their wider families. (Setting standards – donor conception)

Increasing and informing choice: using the data in the register of treatments to improve outcomes and research. (Increasing and informing choice – Register data)

Increasing and informing choice: ensuring that patients have access to high quality meaningful information. (Increasing and informing choice – information)

Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government. (Efficiency, economy and value)

CMG overview – summary from November risk meeting

CMG reviewed the risk register and risk scores at its meeting on 23 November.

CMG updated various risks and scores, and especially discussed IfQ risks – both in the context of strategic risks and related operational risks within teams. The ongoing IfQ work alongside business as usual is undoubtedly causing pressures on resources across the organisation. This was reflected in teams' operational risk logs as well as the strategic risk register. CMG lowered the residual risk for IfQ1, improved information access, since much of the improvement in our engagement channels and information has been completed, and is available in beta. CMG raised the risk level for IfQ3, delivery of promised efficiencies. This risk relates to release two of the clinic portal, incorporating the new electronic data interchange, which is being delayed by competing resource demands from the tail end of release one (website, choose a fertility clinic, and the portal).

Coupled with IfQ delivery, we are going through a period of turnover and internal churn, as a combined result of IfQ contracted resources coming to an end (meaning that staff need to take over their roles), and other incidental turnover. Some internal interim recruitment to bridge gaps has resulted in other recruitment activity to replace or backfill the staff who are moving into different roles. Some of the turnover involves staff with good knowledge of dealing with Parliamentary Questions. Therefore, CMG raised the risk level for Data 2, incorrect data released, and Capability 1, knowledge and capability.

AGC feedback from September meeting

The committee asked the executive to give more consideration to 'plan B' for the website, in the event of an adverse JR judgment, or in the event of Red Dot (the current, outgoing content management system, which was old and unsupported) failing completely.

CMG discussed this issue at its monthly meeting in September, and confirmed that the new website was capable of being used in place of the current website, and that if we needed to deploy it before the JR was resolved, the information under dispute could be removed as a short term measure. The new website made use of a different content management system, Umbraco, which was up to date and supported, as well as more stable and reliable than RedDot. This option meant that our communications channels would remain open, and this seemed sufficient mitigation. In addition, the HFEA had a range of other channels for communicating important information to clinics and other stakeholders, including the clinic portal, social media, Clinic Focus, and email. This was felt to provide a sufficient range of options for important communications should the worst happen and access to the current website be lost.

Authority – November meeting

In the event, the Authority did not actively consider the item, but agreed to note it and submit any comments after the meeting. To date, no comments have been received.

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

Risks are arranged above 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

See last page.

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 does introduce some element of control, even if no other mitigating action were ever taken, and even with no particular risks in mind. Therefore, in order for our estimation of inherent risk to be meaningful, the HFEA defines inherent risk as:

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

System-wide risk interdependencies

We also consider whether any HFEA strategic risks or controls have a potential impact for the Department or any other ALBs.

Risk area	Description and impact	Strategic objective linkage	Risk scores	Recent trend	Risk owner		
Regulatory model RM 1: Quality and safety of care	There is a risk of adverse effects on the quality and safety of care if the HFEA were to fail to deliver its duties under the HFE Act (1990) as amended.	Setting standards: improving the quality and safety of care through our regulatory activities.	Inherent risk level:			↔ ↔ ↔ ↔	Peter Thompson
			Likelihood	Impact	Inherent risk		
			3	5	15 High		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
			2	4	8 Medium		
Tolerance threshold:			8 Medium				
Causes / sources	Mitigations	Timescale and ownership of mitigations	Effectiveness – commentary				
Inspection/reporting failure.	Inspections are scheduled for the whole year, using licence information held on Epicentre, and items are also scheduled to committees well in advance.	In place – Sharon Fensome-Rimmer	At tolerance.				
	Audit of Epicentre conducted to reveal data errors. Queries now routed through Licensing, who hold a definitive list of all licensing details. The correction of errors found is in progress and should be complete shortly.	Audit completed October 2015 – Siobhain Kelly Corrective work in progress for completion in November 2016 – Siobhain Kelly	The Head of Corporate Governance and Chief Inspector started in their posts (in March and May 2016 respectively). The Head of Corporate Governance subsequently left the HFEA in September 2016, leaving a head vacancy again (now filled internally on an interim basis).				
	Inspector training, competency-based recruitment, induction process, SOPs, QMS, and quality assurance all robust.	In place – Sharon Fensome-Rimmer					
Regulatory monitoring processes may be disrupted as a result of the temporary inability of Electronic Patient Record System (EPRS) providers to submit data to the new register structure until their software has been updated. This could impact performance information used in inspection notebooks and RBAT alerts	Proposals on an updated IfQ delivery plan were made to August IfQ Programme Board, these should help address this risk by extending the release date for the EDI replacement by 3 months (IfQ release 2). Mitigation plans for this risk are in the process of being prepared and agreed with SMT as at September.	Mitigation planning in progress in September - Nick Jones	The need to manage recent Heads vacancies, the continuing training period and also the action plan being implemented in connection with legal parenthood consent issues, has raised the residual risk likelihood from 1 (very unlikely) to 2 (unlikely) – through to at least December 2016.				
Monitoring failure.	Outstanding recommendations from inspection reports are tracked and followed up by the team.	In place – Sharon Fensome-Rimmer					
Unresponsiveness to or mishandling of non-compliances or grade A incidents.	Update of compliance and enforcement policy.	Completed following Authority approval of new policy March 2016 - Nick Jones					

	Staffing model provides resilience in the inspection team for such events – dealing with high-impact cases, additional incident inspections, etc.	In place – Sharon Fensome-Rimmer	On legal parenthood, a strong set of actions is in place and continues to be implemented. The issue will also be picked up during the next review of the Code of Practice.
Insufficient inspectors, administrative or licensing staff	Inspection team up to complement. The new Chief Inspector joined the HFEA in early May 2016.	In place – Nick Jones	
	Business support is operating below complement, and this will be addressed shortly, as part of addressing gaps resulting from internal recruitment and churn.	To be addressed shortly – Sharon Fensome-Rimmer	
	Licensing team up to complement following earlier recruitment.	In place – Siobhain Kelly	
Recruitment difficulties and/or high turnover/churn in various areas; resource gaps and resource diversion into recruitment and induction, with impacts felt across all teams.	So far recruitment rounds have yielded sufficient candidates, although this has required going beyond the initial ALB pool to external recruitment in some cases.	Managed as needed – Sharon Fensome-Rimmer	The inspection team continue to work with colleagues in licensed centres where there are anomalies. The focus is on ensuring all affected patients are informed and appropriately supported.
	Additional temporary resources available during periods of vacancy and transition.	In place – Rachel Hopkins	
	Group induction sessions put in place where possible.	In place – Sharon Fensome-Rimmer	
Resource strain itself can lead to increased turnover, exacerbating the resource strain.	Operational performance, risk and resourcing oversight through CMG, with deprioritisation or rescheduling of work an option.	In place – Paula Robinson	
Unexpected fluctuations in workload (arising from eg, very high level of PGD applications received, including complex applications involving multiple types of a condition; high levels of non-compliances either generally or in relation to a particular issue).	Staffing model amended in May 2015, to release an extra inspector post out of the previous establishment. This increased general resilience, enabling more flex when there is an especially high inspection/report writing/application processing workload.	In place – Sharon Fensome-Rimmer	
	Greater sector insight into our PGD application handling processes and decision-making steps achieved in the past few years; coupled with our increased processing rate since efficiency improvements were made in 2013 (acknowledged by the sector).	In place – Sharon Fensome-Rimmer	

Some unanticipated event occurs that has a big diversionary impact on key resources, eg, legal parenthood consent issues, or several major Grade A incidents occur at once.	Resilient staffing model in place.	In place – Sharon Fensome-Rimmer
	Update of compliance and enforcement policy and implementation of new policy and related procedures.	In place – revised policy agreed Spring 2016 – Nick Jones / Sharon Fensome-Rimmer
	<p>A detailed action plan in response to the legal parenthood judgment is in place.</p> <p>There has been correspondence with clinics, who have completed full audits. PRs are responsible for the robustness of the audit.</p> <p>The HFEA has required that clinics support affected patients – using Barts as a good example.</p> <p>In working with clinics, the HFEA has experienced good cooperation. All clinics engaged and have provided assurances about current practice.</p> <p>Through a detailed review of every clinic's responses, a summary list of all concerns is being produced.</p> <p>Management review meetings took place for all clinics at which there are handling concerns or anomalies.</p> <p>Plan of action in place to address all of the concerns identified, with direct follow up with centres who did not respond at all.</p> <p>Where there are engagement concerns, we will do short-notice inspections, focused on parenthood consent.</p> <p>The policy team will develop a range of tools to support licensed clinics in ensuring patients provide effective consent.</p> <p>Range of lessons learned identified.</p>	<p>In progress – Nick Jones/Sharon Fensome-Rimmer</p> <p>Policy team tools – development in 2017/18 business year – Joanne Anton</p>

Risk area	Description and impact	Strategic objective linkage	Risk scores	Recent trend	Risk owner		
Regulatory model RM 2: Loss of regulatory authority	There is a risk that the HFEA could lose authority as a regulator, jeopardising its regulatory effectiveness, owing to a loss of public / sector confidence.	Setting standards: improving the quality and safety of care through our regulatory activities.	Inherent risk level:			⇔ ⇔ ⇔ ⇔	Peter Thompson
			Likelihood	Impact	Inherent risk		
			3	5	15 High		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
			2	4	8 Medium		
Tolerance threshold:			8 Medium				
Causes / sources		Mitigations	Timescale and ownership of mitigations		Effectiveness – commentary		
Failures or weaknesses in decision making processes.		Keeping up to date the standard operating procedures (SOPs) for licensing, representations and appeals.	In place – Siobhain Kelly		At tolerance. Although two additional risk sources exist at present (website outages until the new beta website is live and the plan of work to address legal parenthood consent issues), these are being well managed and/or tolerated, and the overall risk score has not increased.		
		Learning from past representations and Appeal Committee hearings incorporated into processes.	In place – Siobhain Kelly				
		Appeals Committee membership maintained. Ongoing process in place for regular appointments whenever vacancies occur or terms of office end.	In place – Siobhain Kelly				
		Staffing structure for sufficient committee support.	In place – Siobhain Kelly				
		Decision trees; legal advisers familiar.	In place – Siobhain Kelly				
		Proactive management of quoracy for meetings.	In place – Siobhain Kelly				
		New (ie, first application) T&S licences delegated to ELP. Delegations were revisited during 2016 review of Standing Orders. Licensing Officer role to take certain decisions from ELP –the documentation for recording Licensing Officer decisions is complete as at September 2016 and this process is ready for implementation.	In place – Siobhain Kelly Licensing Officer role – ready for implementation September 2016 – Siobhain Kelly Delegations in SOs were put in place - Spring 2016				
Failing to demonstrate competence as a regulator		Update of compliance and enforcement policy and implementation of new policy and related procedures.	In place – revised policy agreed Spring 2016 – Nick Jones / Sharon Fensome-Rimmer				

	Inspector training, competency-based recruitment, induction process, SOPs, quality management system (QMS) and quality assurance all robust.	In place – Sharon Fensome-Rimmer
Effect of publicised grade A incidents.	Staffing model provide resilience in inspection team for such events – dealing with high-impact cases, additional incident inspections, etc.	In place – Sharon Fensome-Rimmer
	SOPs and protocols with Communications team.	In place – Sharon Fensome-Rimmer
	Fairness and transparency in licensing committee information.	In place – Sharon Fensome-Rimmer
	Dedicated section on website, so that the public can openly see our activities in the broader context.	In place – Sharon Fensome-Rimmer
Administrative or information security failure, eg, document management, risk and incident management, data security.	Staff have annual information security training (and on induction).	In place – Dave Moysen
	TRIM training and guidance/induction in records management in place pending new work on records management to be commenced in autumn 2016 (see below).	New work in development as at September 2016
	Further work planned on records management in parallel with IT strategy. This piece of work is currently being scoped.	Linked to IT strategy work – in progress – Siobhain Kelly / David Moysen
	Guidance/induction in handling FOI requests, available to all staff.	In place – Siobhain Kelly
	The IfQ website management project has reviewed the retention schedule.	Completed – August 2015 – Juliet Tizzard
Until the IfQ website project has been completed, there is a continued risk of HFEA website outages, as well as difficulties in uploading updates to web pages.	Alternative mechanisms are in place for clinics to get information about materials such as the Code of Practice (eg, direct communications with inspectors, Clinic Focus).	In place – Sharon Fensome-Rimmer
	The IfQ work on the new website will completely mitigate this risk (the new content management system will remove the current instability we are experiencing from using RedDot). This risk has informed our decisions about which content to move first to the beta version of the new site.	In progress – beta phase February 2016 – Juliet Tizzard

Negative media or criticism from the sector in connection with legally disputed issues or major adverse events at clinics.	HFEA approach is only to go into cases on the basis of clarifying legal principles or upholding the standards of care by challenging poor practice. This is more likely to be perceived as proportionate, rational and necessary (and impersonal), and is in keeping with our strategic vision.	In place - Peter Thompson
HFEA process failings that create or contribute to legal challenges, or which weaken cases that are otherwise sound, or which generate additional regulatory sanctions activity (eg, legal parenthood consent).	Licensing SOPs, committee decision trees in place. Mitochondria donation application tools completed.	In place – Siobhain Kelly
	Update of compliance and enforcement policy and implementation of new policy and related procedures.	In place – revised policy agreed Spring 2016 – Nick Jones / Sharon Fensome-Rimmer
	Seeking the most robust possible assurance from the sector with respect to legal parenthood consent issues, and detailed plan in operation to address identified cases and anomalies.	In progress – Nick Jones
	QMS and quality assurance in place in inspection team.	In place – Sharon Fensome-Rimmer

Risk area	Description and impact	Strategic objective linkage	Risk scores	Recent trend	Risk owner		
IfQ IfQ 1: Improved information access	If the information for Quality (IfQ) programme does not enable us to provide better information and data, and improved engagement channels, patients will not be able to access the improved information they need to assist them in making important choices.	Increasing and informing choice: ensuring that patients have access to high quality meaningful information.	Inherent risk level:			↔ ↔ ↔ ↓	Juliet Tizzard
			Likelihood	Impact	Inherent risk		
			4	4	16 High		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
2	4	8 Medium					
Tolerance threshold:			8 Medium				
Causes / sources		Mitigations	Timescale and ownership of mitigations		Effectiveness – commentary		
Inability to extract reliable data from the Register.		Detailed planning and programme management in place to ensure this will be possible after migration. Migration strategy developed, and significant work being done to identify and cleanse all of the data that requires correction before migration. Decisions have been made about the degree of reliability required in each data field. For those fields where 100% reliability is needed, inaccurate or missing data is being addressed as part of project delivery.	All aspects – detailed project planning in place – Nick Jones		At tolerance. The approval process has had to be tightly managed; a summary is set out below. The first Department of Health gateway review took place in November 2015 and awarded a high score to the HFEA, but the formal decision on this was still not made by the Government Digital Service board until mid-January (a month later than expected). This meant that the beta (build) stage initially had to proceed at risk (subsequently resolved).		
Reduced ability to provide for patient choice based on CaFC information as a result of EPRS inability to submit/correct data in the new register structure if they do not update their systems in time to comply. This could impact the publication of CaFC data.		Proposals on an updated IfQ delivery plan were agreed at August IfQ Programme Board, these should help address this risk. A mitigation and communication plan for this risk is in place, including ongoing dialogue with EPRS centres and providers.	In place - Nick Jones				

Stakeholders dislike or fail to accept the new model for CaFC. Stakeholders not on board with the changes.	In-depth stakeholder engagement and extensive user research completed to inform the programme's intended outcomes, products and benefits. This included, consultation, expert groups and Advisory Board and this continues to be an intrinsic part of programme approach.	In place and ongoing – Juliet Tizzard /Nick Jones	Approval also carried a number of requirements and conditions which need to be added to the delivery. Owing to these delays, it was necessary to extend the timeline for the private beta phase from March to June 2016.
Cost of delivering better information becomes too prohibitive, either because the work needed is larger than anticipated, or as a result of the approval periods associated with required DH/GDS gateway reviews.	Costs were taken into account as an important factor in consideration of contract tenders and negotiations. Following earlier long timelines and unsuccessful attempts to discuss with GDS, our experience at the Beta gateway has been much improved and feedback was almost immediate. Watching brief being kept.	In place – Nick Jones In place – Nick Jones	The live beta gateway approval in May was much more efficient, with approvals received within days of the assessment taking place. However, there were a number of requirements to address before implementing live beta.
Redeveloped website does not meet the needs and expectations of our various user types.	Programme approach and some dedicated resources in place to manage the complexities of specifying web needs, clarifying design requirements and costs, managing changeable Government delegation and permissions structures, etc. User research done, to properly understand needs and reasons. Tendering and selection process included clear articulation of needs and expectations. GDS Beta assessment was passed on all 18 points.	In place – user research delivered end Oct 2016 – Juliet Tizzard	The move to public beta was delayed by an injunction brought by a licensed clinic. We successfully managed to have the injunction lifted, but it meant that we could not issue the new website to public beta testing until August 2016. Due partly to this, the timeline was extended further, with additional work impacting on the planned start-up of release two work, and on the timelines for go live GDS assessments for both the portal and the website.
Government and DH permissions structures are complex, lengthy, multi-stranded, and sometimes change mid-process.	Initial external business cases agreed and user research completed. Final business case for whole IfQ programme was submitted and eventually accepted. All GDS approvals sought so far have been granted, albeit with some delays to the earlier ones. Additional sprints of work were incorporated in beta, in an attempt to allow sufficient time (and resources) for the remaining GDS gateway review processes and subsequent formal approval mechanisms. The beta timeline was extended by 3 months to	In place – Juliet Tizzard In place – Nick Jones (decision received April 2015) In place – Nick Jones	The GDS go live assessment for the portal subsequently took place in November. No date has

	compensate for previous and anticipated future delays.		yet been set for the go live gateway assessment for the website.
Resource conflicts between delivery of website and business as usual (BAU).	Backfilling where possible/affordable to free up the necessary staff time, eg, Websites and Publishing Project Manager post backfilled to free up core staff for IfQ work.	In place – Juliet Tizzard	
Delivery quality is very supplier dependent. Contractor management could become very resource-intensive for staff, or the work delivered by one or more suppliers could be poor quality and/or overrun, causing knock-on problems.	Programme management resources and quality assurance mechanisms in place for IfQ to manage (among other things) contractor delivery. Agile project approach includes a 'one team' ethos and requires close joint working and communication among all involved contractors. Sound project management practices in place to monitor delivery. Previous lessons learned and knowledge exist in the organisation from managing some previous projects where poor supplier delivery was an issue requiring significant hands-on management. Ability to consider deprioritising other work, through CMG, if necessary. Regular contract meetings in place. This remains a challenge.	In place – Juliet Tizzard	
New CMS (content management software) is ineffective or unreliable.	CMS options were scrutinised carefully as part of project. Appropriate new CMS chosen, and all involved teams happy with the selection.	In progress – implemented in beta phase, July 2016 – Juliet Tizzard	
Benefits not maximised and internalised into ways of working.	During IfQ delivery, product owners are in place, as is a communications plan. The aim is to ensure that changes are developed involving the right staff expertise (as well as contractors) and to ensure that the changes are culturally embraced and embedded into new ways of working. Knowledge handover with the contractors will take place.	In place – Nick Jones	

Risk area	Description and impact	Strategic objective linkage	Risk scores	Recent trend	Risk owner		
IfQ IfQ 2: Register data	HFEA Register data becomes lost, corrupted, or is otherwise adversely affected during IfQ programme delivery.	Increasing and informing choice: using the data in the Register of Treatments to improve outcomes and research.	Inherent risk level:			↔ ↔ ↔ ↔	Nick Jones
			Likelihood	Impact	Inherent risk		
			2	5	10 Medium		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
			2	4	8 Medium		
Tolerance threshold:			8 Medium				
Causes / sources		Mitigations	Timescale and ownership of mitigations		Effectiveness – commentary		
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		At tolerance. This risk is being intensively managed – a major focus of IfQ detailed planning work, particularly around data migration.		
The firm (Avoca) which was scheduled to provide assurance on data migration has gone out of business.		The HFEA has considered other sources of assurance and have now sourced a supplier and is currently going through procurement processes to appoint them.	Pending a successful appointment process, we would expect the new company to begin providing assurance in September/October– Nick Jones				
Historic data cleansing is needed prior to migration.		A detailed migration strategy is in place, and data cleansing is in progress.	In place – Nick Jones/Dave Moysen				
Increased reporting needs mean we later discover a barrier to achieving this, or that an unanticipated level of accuracy is required, with data or fields which we do not currently focus on or deem critical for accuracy.		IfQ planning work incorporated consideration of fields and reporting needs were agreed. Decisions about the required data quality for each field were 'future proofed' as much as possible through engagement with stakeholders to anticipate future needs and build these into the design.	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				
System interdependencies change / are not recognised		Strong interdependency mapping done between IfQ and business as usual.	Done – Nick Jones				
Benefits not maximised and internalised		During IfQ delivery, product owners are in place, as	In place – Nick Jones				

<p>into ways of working.</p>	<p>is a communications plan. The aim is to ensure that changes are developed involving the right staff expertise (as well as contractors) and to ensure that the changes are culturally embraced and embedding into new ways of working. Knowledge handover with the contractors will take place.</p>	
------------------------------	---	--

Risk area	Description and impact	Strategic objective linkage	Risk scores	Recent trend	Risk owner	
IfQ IfQ 3: Delivery of promised efficiencies	There is a risk that the HFEA's promises of efficiency improvements in Register data collection and submission are not ultimately delivered.	Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government.	Inherent risk level:			↔ ↓ ↔ ↑ Nick Jones
			Likelihood	Impact	Inherent risk	
			4	4	16 High	
			Residual risk level:			
			Likelihood	Impact	Residual risk	
			3	4	12 High	
Tolerance threshold:			9 Medium			
Causes / sources		Mitigations	Timescale and ownership of mitigations		Effectiveness – commentary	
Poor user acceptance of changes, or expectations not managed.		Stakeholder involvement strategy in place and user testing being incorporated into implementation phases of projects.	In place – Nick Jones/Juliet Tizzard		Above tolerance.	
Clinics not consulted/involved enough.		Working with stakeholders has been central to the development of IfQ, and will continue to be. Advisory Group and expert groups have ended, but a stakeholder group for the implementation phase is in place. Workshops were delivered with the sector regarding how information will be collected through the clinic portal. From beta live onwards we will receive feedback and iteratively develop the products.	In place – Nick Jones/Juliet Tizzard		In September 2016, since we believed that the mitigations that are in place are working effectively and mean that we are on track to achieve the promised efficiencies, we reduced the level of likelihood for this risk. This in turn brought the risk to below the tolerance threshold of 9.	
Scoping and specification are insufficient for realistic resourcing and on-time delivery of changes.		Scoping and specification were elaborated with stakeholder input, so as to inform the tender. Resourcing and timely delivery were a critical part of the decision in awarding the contract.	In place and contracts awarded (July 2015) – Nick Jones		This risk is also affected by GDS approvals and associated requirements (see IfQ1).	
Efficiencies cannot, in the end, be delivered.		Detailed scoping phase included stakeholder input to identify clinic users' needs accurately. Specific focus in IfQ projects on efficiencies in data collected, submission and verification, etc.	In place – Nick Jones		In November 2016, in light of delays to release two of the portal (which includes the new electronic data interchange system for data submission by clinics), we increased this risk again. The delays stem from the	
Cost of improvements becomes too prohibitive, or resources are insufficient to complete the Programme.		Contracts only awarded to bidders who made an affordable proposal. Detailed planning for release two (which includes the second iteration of the portal and the	In place (July 2015) – Nick Jones In progress (September 2016) – Nick Jones			

	<p>introduction of the new EDI interface) is in progress and the HFEA will continue to work within agreed costs.</p> <p>A contingency amount was built into the budget, although this has now been used.</p> <p>The support function is being re-shaped and streamlined to deal with the departure in November of the release two project manager.</p>	<p>In progress (November 2016) – Nick Jones</p>	<p>ongoing work still needed on release one, which requires the attention of the same staff who are needed for release two. In addition, some key IfQ contracted staff are coming to the end of their contracts with work still ongoing.</p>
<p>Delivery is delayed, causing reputational damage to the HFEA.</p>	<p>Ongoing communication with clinics via Clinic Focus and direct correspondence, to keep them up to date and make them aware of delays.</p>	<p>In place – Nick Jones</p>	
<p>Required GDS gateway approvals are delayed or approval is not given.</p>	<p>All GDS approvals sought so far have been granted, albeit with some delays to earlier gateways.</p> <p>Our detailed planning includes addressing the requirements laid down by GDS as conditions of alpha and beta phase approval.</p> <p>Additional sprints of work were incorporated into beta, in an attempt to allow sufficient time (and resources) for the remaining GDS gateway review processes and subsequent formal approval mechanisms.</p> <p>The beta timeline was extended by 3 months to compensate for previous and anticipated future delays.</p>	<p>In place – Nick Jones</p>	
<p>Benefits not maximised and internalised into ways of working.</p>	<p>During IfQ delivery, product owners are in place, as is a communications plan. The aim is to ensure that changes are developed involving the right staff expertise (as well as contractors) and to ensure that the changes are culturally embraced and embedded into new ways of working.</p> <p>Knowledge handover with the contractors will take place.</p>	<p>In place (June 2015) – Nick Jones</p>	

Risk area	Description and impact	Strategic objective linkage	Risk scores	Recent trend	Risk owner		
Legal challenge LC 1: Resource diversion	There is a risk that the HFEA is legally challenged in such a way that resources are significantly diverted from strategic delivery.	Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government.	Inherent risk level:			↓ ↔ ↔ ↔	Peter Thompson
			Likelihood	Impact	Inherent risk		
			5	4	20 Very high		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
			4	3	12 High		
Tolerance threshold:			12 High				
Causes / sources		Mitigations	Timescale and ownership of mitigations		Effectiveness – commentary		
Complex and controversial area.		Panel of legal advisors from various firms at our disposal for advice, as well as in-house Head of Legal.	In place – Peter Thompson		At tolerance. Current cases: The judgment in 2015 and subsequent cases on consents for parenthood have administrative and policy consequences for the HFEA. Further cases are going through court, although there have been no cases arising from new incidents post the 2015 judgment. The HFEA is unlikely to participate in most of these legal proceedings directly, though the court has required us to provide information and clarification in relation to six legal parenthood cases. A judicial review hearing of one discrete element of the IfQ CaFC project has been set for December. Authority decisions in November may impact on the scope of the JR. We are advised that our case is strong;		
		Evidence-based policy decision-making and horizon scanning for new techniques.	In place – Joanne Anton				
		Robust and transparent processes in place for seeking expert opinion – eg, external expert advisers, transparent process for gathering evidence, meetings minuted, papers available online.	In place – Joanne Anton/Juliet Tizzard				
HFE Act and regulations lead to the possibility of there being differing legal opinions from different legal advisers, that then have to be decided by a court.		Panel in place, as above, to get the best possible advice. Case by case decisions regarding what to argue in court cases, so as to clarify the position.	In place – Peter Thompson				
Decisions and actions of the HFEA and its committees may be contested. 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.		Panel in place, as above.	In place – Peter Thompson				
		Maintaining, keeping up to date and publishing licensing SOPs, committee decision trees etc. consistent decision making at licence committees supported by effective tools for committees Standard licensing pack completely refreshed and distributed to members/advisers (April 2015).	In place – Siobhain Kelly				
		Well-evidenced recommendations in inspection reports.	In place – Sharon Fensome-Rimmer				
Subjectivity of judgments means the		Scenario planning is undertaken at the initiation of	In place – Peter Thompson				

HFEA often cannot know in advance which way a ruling will go, and the extent to which costs and other resource demands may result from a case.	any likely action.		however, if it were lost then it may impact on aspects of the presentation of data.
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 interdependent risk because DH would be involved in resolving it.	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 – Siobhain Kelly	

Risk area	Description and impact	Strategic objective linkage	Risk scores	Recent trend		
Data D 1: Data loss or breach	There is a risk that HFEA data is lost, becomes inaccessible, is inadvertently released or is inappropriately accessed.	Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government.	Inherent risk level:			⇔ ⇔ ⇔ ⇔
			Likelihood	Impact	Inherent risk	
			4	5	20 Very high	
			Residual risk level:			
			Likelihood	Impact	Residual risk	
			2	5	10 Medium	
Tolerance threshold:			10 Medium			
Causes / sources		Mitigations	Timescale and ownership of mitigations	Effectiveness – commentary		
Confidentiality breach of Register data.		Staff have annual compulsory security training to guard against accidental loss of data or breaches of confidentiality. Secure working arrangements for Register team, including when working at home.	In place – Dave Moysen	At tolerance.		
Loss of Register or other data.		As above. 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			
Cyber-attack and similar external risks.		Secure system in place as above, with regular penetration testing.	In place – Dave Moysen			
Infrastructure turns out to be insecure, or we lose connection and cannot access our data.		IT strategy agreed, including a thorough investigation of the Cloud option, security, and reliability.	In place – Dave Moysen			
		Deliberate internal damage to infrastructure, or data, is controlled 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.		BCP in place and staff communication procedure	In place – Richard Sydee			

	tested. A new BCP is being produced by the Head of IT to reflect the changes to this following changes to infrastructure and the office move.	Update done Dave Moysen – September 2016	
Register data becomes corrupted or lost somehow.	Back-ups and warehouse in place to ensure data cannot be lost.	In place – Nick Jones/Dave Moysen	
Other HFEA data (system or paper) is lost or corrupted.	As above. Staff have annual compulsory security training to guard against accidental loss of data or breaches of confidentiality.	In place – Dave Moysen	
Poor records management	TRIM training and guidance/induction in records management in place pending new work on records management to be commenced in autumn 2016 (see below). New work in development as at September 2016	New work in development as at September 2016	
	Further work planned on records management in parallel with IT strategy. This piece of work is currently being scoped. Linked to IT strategy work – in progress – Siobhain Kelly / David Moysen	Linked to IT strategy work – in progress – Siobhain Kelly / David Moysen	

Risk area	Description and impact	Strategic objective linkage	Risk scores	Recent trend	Risk owner		
Data D 2: Incorrect data released	There is a risk that incorrect data is released in response to a Parliamentary question (PQ), or a Freedom of Information (FOI) or data protection request.	Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government.	Inherent risk level:			↔ ↔ ↔ ↑	Juliet Tizzard
			Likelihood	Impact	Inherent risk		
			5	4	20 Very high		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
			3	4	12 High		
Tolerance threshold:			8 Medium				
Causes / sources		Mitigations	Timescale and ownership of mitigations		Effectiveness – commentary		
Poor record keeping		Refresher training and reminders about good records management practice.	In place – SMT		Above tolerance. Although we have some good controls in place for dealing with PQs and other externally generated requests, it should be noted that we cannot control incoming volumes, complexity or deadlines. In September 2016 we have not yet registered an unusual spike in volumes following on from recess (during which time there were no PQs). However, with the current work on the mitochondria scientific review, due to be published in December, this situation is likely to change in future months. We continue to closely monitor volumes.		
		TRIM review and retention policy implementation work – part of records management project	To sync in with IT strategy. RM project to start autumn 2016 – Dave Moysen/Siobhain Kelly				
		Audit of Epicentre to reveal any data errors. All queries being routed through Licensing, who have a definitive list of all licensing details.	Completed October 2015 – Siobhain Kelly Implementation of actions following Epicentre audit planned and to be completed by November 2016– Siobhain Kelly				
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. If more time is needed for a complex PQ, it is occasionally necessary to take the issue out of the very tightly timed PQ process and replace this with a more detailed and considered letter back to the enquirer so as to provide the necessary level of detail and accuracy in the answer. We also refer back to previous answers so as to give a check, and to ensure consistent presentation of similar data. FOI requests are refused when there are grounds for this.	In place – Juliet Tizzard / Nick Jones				

	PQ SOP revised and log created, to be maintained by Committee and Information Officer/Scientific Policy Manager.	In place - Siobhain Kelly
Staff turnover resulting in the loss of corporate knowledge regarding the history and handling of PQs, in particular, resulting in slower handling and therefore potential reputational effect with the Department of Health.	Staff have access to past records to inform new responses. Recruitment in progress. Additional legal advice will be sought when beneficial. Good lines of communication with the Department so that any difficulties can be highlighted at the earliest possible point.	In place – Siobhain Kelly Recruitment in progress – Siobhain Kelly
Answers in Hansard may not always reflect advice from HFEA.	The PQ team attempts to catch any changes to drafted wording that may unwittingly have changed the meaning. HFEA's suggested answer and DH's final submission both to be captured in new PQ log.	In place – Siobhain Kelly / Peter Thompson
Insufficient understanding of underlying system abilities and limitations, and/or of the topic or question, leading to data being misinterpreted or wrong data being elicited.	As above – expert staff with the appropriate knowledge and understanding in place.	In place – Juliet Tizzard / Nick Jones
Servicing data requests for researchers - poor quality of consents obtained by clinics for disclosure of data to researchers.	There is a recognised risk of centres reporting research consents inaccurately. Work is ongoing to address consent reporting issues	Inspections now routinely sample check a clinic's performance comparing original consent form with the detail held on the Register, to ensure it has been transcribed effectively. Where the error rate is above tolerance the clinic must undertake a full audit and carry out corrections to the Register as necessary – Nick Jones

Risk area	Description and impact	Strategic objective linkage	Risk scores	Recent trend	Risk owner		
Donor conception DC 1: OTR inaccuracy	There is a risk that an OTR applicant is given incorrect data.	Setting standards: improving the lifelong experience for donors, donor-conceived people, patients using donor conception, and their wider families.	Inherent risk level:			↔ ↔ ↔ ↔	Nick Jones
			Likelihood	Impact	Inherent risk		
			3	5	15 High		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
			1	4	4 Low		
Tolerance threshold:			4 Low				
Causes / sources		Mitigations	Timescale and ownership of mitigations		Effectiveness – commentary		
Data accuracy in Register submissions.		Continuous work with clinics on data quality, including current verification processes, steps in the OTR process, regular audit alongside inspections, and continued emphasis on the importance of life-long support for donors, donor-conceived people and parents.	In place – Nick Jones		At tolerance (which is very low for this risk).		
		Audit programme to check information provision and accuracy.	In place – Nick Jones				
		IfQ work will identify data accuracy requirements for different fields as part of the migration process, and will establish 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				
Issuing of wrong person's data.		OTR process has an SOP that includes specific steps to check the information given and that it relates to the right person.	In place – Nick Jones				
Process error or human error.		As above.	In place – Nick Jones				

Risk area	Description and impact	Strategic objective linkage	Risk scores	Recent trend	Risk owner		
Donor conception DC 2: Support for OTR applicants	There is a risk that inadequate support is provided for donor-conceived people or donors at the point of making an OTR request.	Setting standards: improving the lifelong experience for donors, donor-conceived people, patients using donor conception, and their wider families.	Inherent risk level:			↔ ↔ ↔ ↔	Nick Jones
			Likelihood	Impact	Inherent risk		
			4	4	16 High		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
			3	3	9 Medium		
Tolerance threshold:			9 Medium				
Causes / sources		Mitigations	Timescale and ownership of mitigations		Effectiveness – commentary		
Lack of counselling availability for applicants.		Counselling service established with external contractor in place.	In place (June 2015) – Nick Jones		At tolerance.		
Insufficient Register team resource to deal properly with OTR enquiries and associated conversations.		Additional member of staff dedicated to handling such enquiries. However, there is currently also one member of staff returning to work from long term sick leave, and this together with work pressures from IfQ delivery means there is still some pressure on team capacity (being discussed by managers).	In place, with ongoing team capacity issue under discussion – Nick Jones		The pilot counselling service has been in place since 1 June 2015, and we will make further assessments based on uptake and the delivery experience. Reporting to the Authority will occur annually during the pilot period, and the first such report was provided to the July Authority meeting.		
Risk of inadequate handling of a request.		Trained staff, SOPs and quality assurance in place.	In place – Nick Jones				
		SOPs reviewed by Register staff, CMG and PAC-UK, as part of the pilot set-up. Contract in place with PAC-UK for pilot delivery.	Done (May 2015) – ongoing management of the pilot by Rosetta Wotton.				

Risk area	Description and impact	Strategic objective linkage	Risk scores	Recent trend	Risk owner		
Financial viability FV 1: Income and expenditure	There is a risk that the HFEA could significantly overspend (where significantly = 5% of budget, £250k)	Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government.	Inherent risk level:			↔ ↔ ↔ ↔	Richard Sydee
			Likelihood	Impact	Inherent risk		
			4	4	16 High		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
			3	3	9 Medium		
Tolerance threshold:			9 Medium				
Causes / sources		Mitigations	Timescale and ownership of mitigations		Effectiveness – commentary		
Fee regime makes us dependent on sector activity levels.		Activity levels are tracked and change is discussed at CMG, who would consider what work to deprioritise and reduce expenditure.	Monthly (on-going) – Morounke Akingbola		At tolerance. 2015/16 achieved a small under-spend but risk of additional legal costs remains.		
		Fees Group created enabling dialogue with sector about fee levels. Fee increase was agreed and approved by Treasury. This was implemented and the eSET discount ended (April 2016).	In place. Fees Group meeting in October, ongoing – Morounke Akingbola		The increase of per-cycle fees by £5 (to £80) and the end of the small 'eSET discount' for elective single embryo transfer has now been implemented following Treasury approval in February 2016. This should help secure sufficient funds going forward.		
EPRS suppliers may not make required changes to their systems in line with IfQ data submission mechanism (EDI, Register) changes. Clinics using these suppliers would be unable to provide treatment data leading to deferral of fee payment since we could not bill centres for treatments.		Proposals were made to August IfQ Programme Board for adjustments to the IfQ schedule which would impact when this risk is likely to be felt. Further discussions are needed with Finance to understand the scale of the potential impact of this risk and to plan for an effective mitigation to secure cash flow. These discussions will be ongoing while IfQ release 2 develops further.	Ongoing -Nick Jones		It is too early for us to tell whether this reduces this risk further. The situation will be clearer following IfQ implementation.		
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.	Quarterly meetings (on-going) – Morounke Akingbola		The potential impact of the IfQ risk here, related to EPRS suppliers and the impact on treatment fees, is not yet fully		
		Annual budget agreed with DH Finance team alongside draft business plan submission.	December annually – Morounke Akingbola				
		Detailed budgets for 2016/17 have been agreed with Directors. DH has previously agreed our resource envelope.	In place – Morounke Akingbola				

Budget setting process is poor due to lack of information from directorates	Quarterly meetings with directorates flags any shortfall or further funding requirements.	Quarterly meetings (on-going) – Morounke Akingbola	understood. It is also clear that this would not potentially impact the organisation until 2017, so the risk level is not affected at this time. Meanwhile, the IfQ team will work together closely with the finance team and the mitigation for this risk will be updated once more information is gathered and a plan agreed. We will keep this under review.
Unforeseen increase in costs eg, legal, IfQ or extra in-year work required	Use of reserves, up to contingency level available. DH kept abreast of current situation and are a final source of additional funding if required. IfQ Programme Board regularly reviews the budget and costs.	Monthly – Morounke Akingbola Monthly – IfQ Programme Board	
Upwards scope creep during projects, or emerging during early development of projects eg, IfQ.	Periodic review of actual and budgeted spend by IfQ project board and monthly budget meetings with finance. Cash flow forecast updated.	Ongoing – Wilhelmina Crown Monthly (on-going) – Morounke Akingbola	

Risk area	Description and impact	Strategic objective linkage	Risk scores	Recent trend	Risk owner		
Capability C 1: Knowledge and capability	There is a risk that the HFEA experiences unforeseen knowledge and capability gaps, threatening delivery of the strategy.	Efficiency, economy and value: ensuring the HFEA remains demonstrably good value for the public, the sector and Government.	Inherent risk level:			⇔ ⇔ ⇔ ↑	Peter Thompson
			Likelihood	Impact	Inherent risk		
			4	4	16 High		
			Residual risk level:				
			Likelihood	Impact	Residual risk		
			4	3	12 High		
Tolerance threshold:			6 Medium				
Causes / sources		Mitigations	Timescale and ownership of mitigations		Effectiveness – commentary		
High turnover, sick leave etc. leading to temporary knowledge loss and capability gaps.		People strategy will partially mitigate. Mixed approach of retention, staff development, and effective management of vacancies and recruitment processes.	Done – May 2015 – Rachel Hopkins		Above tolerance. This risk and the set of controls remains focused on capability, rather than capacity. There are obviously some linkages, since managing turnover and churn also means managing fluctuations in capability and ensuring knowledge and skills are successfully nurtured and/or handed over. Since the HFEA is a small organisation, with little intrinsic resilience, it seems prudent to retain a low tolerance level for this risk. Our Head vacancies earlier in 2016, in Licensing and Compliance, were initially filled (in March and May 2016 respectively). However the Head of Corporate Governance subsequently left in September 2016, and has been replaced		
		Staff have access to civil service learning (CSL); organisational standard is five working days per year of learning and development for each member of staff.	In place – Rachel Hopkins				
		Organisational knowledge captured via records management (TRIM), case manager software, project records, 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				
The new UK 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.		The HFEA was proactive in reducing its headcount and other costs to minimal levels over a number of years. We have also been reviewed extensively (including the McCracken review). Turnover is variable, and so this risk will be retained on the risk register, and will continue to receive ongoing management attention.	In place – Peter Thompson				
Poor morale leading to decreased		Engagement with the issue by managers. Ensuring	In place – Peter Thompson				

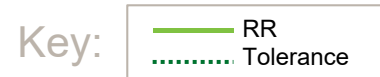
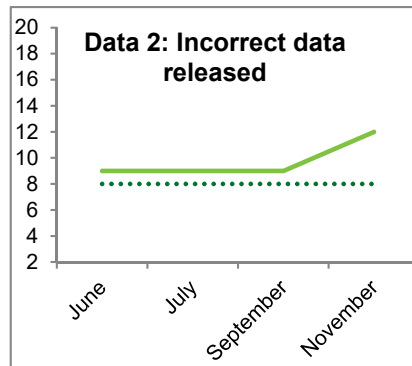
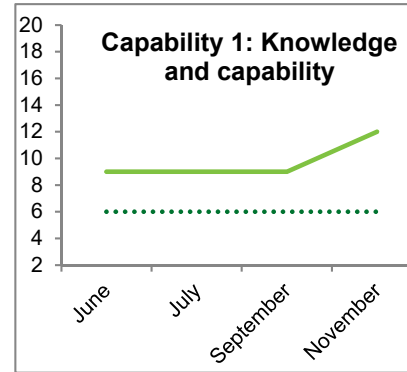
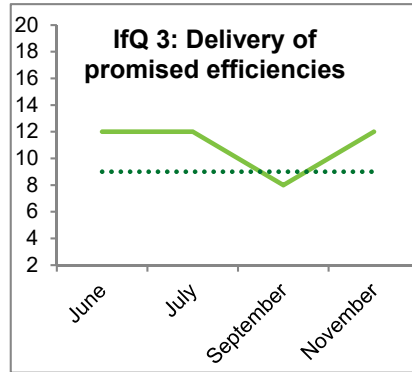
effectiveness and performance failures.	managers have team meetings and one-to-one meetings to obtain feedback and identify actions to be taken.		internally on an interim basis, with associated recruitment activity needed in the team. Several staff (including end of contract IfQ staff) have left the organisation recently, with two more establishment staff leaving before the end of the year. This means we are currently in a period of turnover and internal churn, with some knowledge gaps, and IfQ work ongoing for both release one and release two.
	Staff survey and implementation of outcomes, following up at December 2015 all staff conference.	Survey and staff conference done – Rachel Hopkins Follow-up communications in place (Staff Bulletin etc.) – Peter Thompson	
Differential impacts of IfQ-related change and other pressures for particular teams could lead to specific areas of knowledge loss and low performance.	Staff kept informed of likely developments and next steps, and when applicable of personal role impacts and choices.	In place – Nick Jones	
	Policies and processes to treat staff fairly and consistently, particularly if people are 'at risk'.	In place – Peter Thompson	
Additional avenues of work open up, or reactive diversions arise, and need to be accommodated alongside the major IfQ programme.	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	
	Early emphasis given to team-level service delivery planning, with active involvement of team members. CMG will continue to review planning and delivery.	In place – Paula Robinson	
	Planning for 2016/17 prioritises IfQ delivery, and therefore strategy delivery, within our limited resources.	In place as part of business planning (2015 onwards) – Paula Robinson	
	IfQ has some of its own dedicated resources.	In place – Nick Jones	
	There is a degree of flexibility within our resources, and increasing resilience is a key consideration whenever a post becomes vacant. Staff are encouraged to identify personal development opportunities with their manager, through the PDP process, making good use of CSL.	In place – Peter Thompson	
Regarding the recent work on licensing mitochondrial replacement techniques, there is a possible future risk that we will	Future needs (capability and capacity) relating to mitochondrial replacement techniques and licensing applications are starting to be considered now, but	Issue for consideration when applications commence – Juliet Tizzard	

need to increase both capability and capacity in this area, depending on uptake (this is not yet certain).

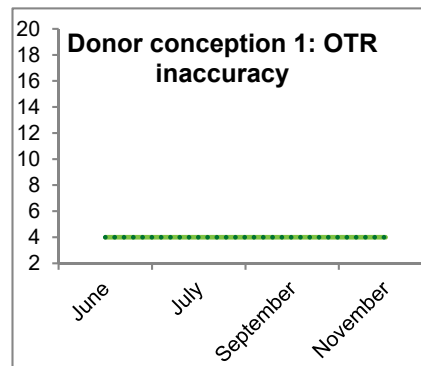
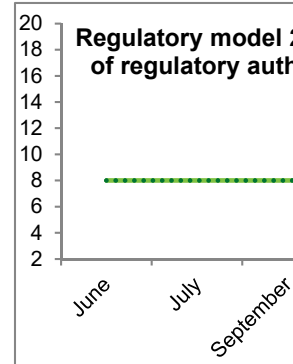
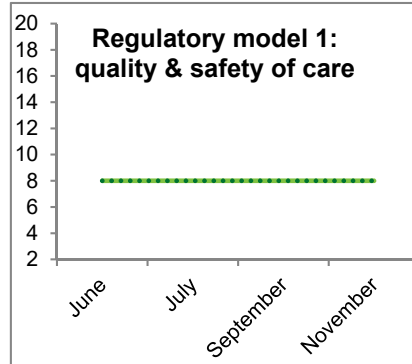
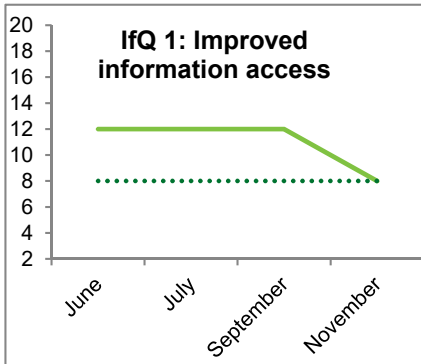
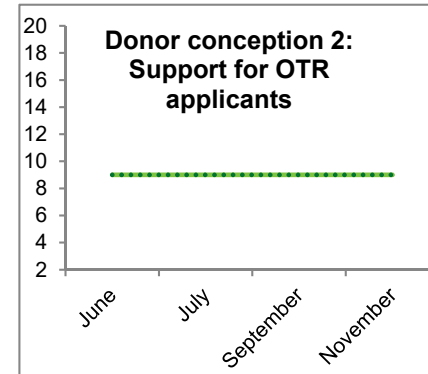
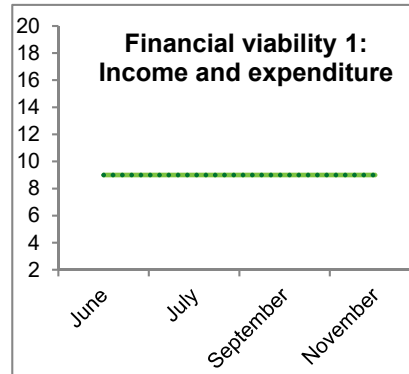
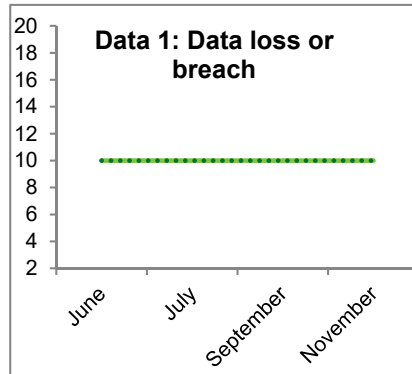
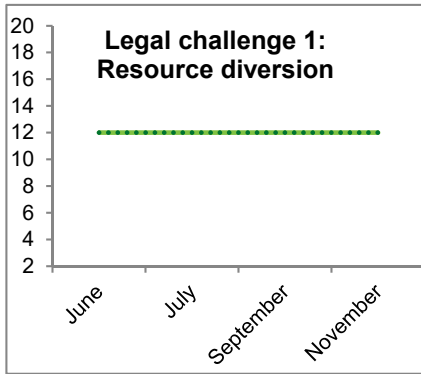
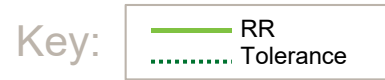
will not be known for sure until later. No controls can yet be put in place, but the potential issue is on our radar.

Tolerance vs Residual Risk:

Risks above tolerance



Risks at tolerance



Risk below tolerance

None.

Scoring system

The HFEA uses the five-point rating system when assigning a rating to both the likelihood and impact of individual risks:

Likelihood: 1=Very unlikely 2=Unlikely 3=Possible 4=Likely 5=Almost certain

Impact: 1=Insignificant 2=Minor 3=Moderate 4=Major 5=Catastrophic

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

Health Group Internal Audit

INTERNAL AUDIT PROGRESS REPORT DECEMBER 2016

Health Group Internal Audit provides an objective and independent assurance, analysis and consulting service to the Department of Health and its arm's length bodies, bringing a disciplined approach to evaluating and improving the effectiveness of risk management, control and governance processes.

The focuses on business priorities and key risks, delivering its service through three core approaches across all corporate and programme activity:

- **Review and evaluation** of internal controls and processes;
- **Advice to support management** in making improvements in risk management, control and governance; and
- **Analysis of policies, procedures and operations** against good practice.

Our findings and recommendations:

- Form the basis of an independent opinion to the Accounting Officers and Audit Committees of the Department of Health and its arm's length bodies on the degree to which risk management, control and governance support the achievement of objectives; and
- Add value to management by providing a basis and catalyst for improving operations.

Our work has been conducted and our report prepared solely for the benefit of the Department of Health and its arm's length bodies and in accordance with a defined and agreed terms of reference. In doing so, we have not taken into account the considerations of any third parties. Accordingly, as our report may not consider issues relevant to such third parties, any use they may choose to make of our report is entirely at their own risk and we accept no responsibility whatsoever in relation to such use. Any third parties, requiring access to the report may be required to sign 'hold harmless' letters.

For further information please contact:
Cameron Robson - 01132 54 6083
1N16 Quarry House, Quarry Hill,
Leeds, LS2 7UE

<u>CONTENTS</u>	<u>PAGE</u>
1. Introduction	1
2. Progress against 2016/17 Internal Audit Plan	1
2.1 Status of agreed plan	1
2.2 Summary of reports issued since the last Audit and Governance Committee	4
2.3 Follow up work	4
2.4 Impact on Annual Governance Statement	4
Appendix 1: Report Rating Definitions	5
Appendix 2: Limitations and responsibilities	6

HFEA Internal Audit Progress Report December 2016

1) Introduction

This paper sets out the progress in completing the 2016/17 Internal Audit Plan since the last meeting of the Audit and Governance Committee in September 2016.

2) Progress against 2016/17 Internal Audit Plan

2.1 Status of agreed plan:

The table below summarises the progress against each of the review areas in the 2016/17 Audit Plan:

Reviews per 201/17 IA plan	Audit scope	Status	Findings			Overall report rating	Audit days per plan	Actual audit days
			High	Medium	Low			
Income generation process	These reviews were merged into one as they both focused on the revenue process. We mapped the income generation and invoicing process from receipt of the electronic treatment forms from clinics to the raising of an invoice. In addition, we evaluated the design and operating effectiveness of controls over the data being used within the income process, considering the mechanisms to ensure that the original source data is of appropriate quality to support invoicing and the checks in place to ensure that integrity of data is maintained during the income and invoicing process. Management also requested that we review the risk management process in place in	Final report issued September 2016	0	1	4	Moderate	5	9
Quality and efficiency of revenue data							4	

Reviews per 201/17 IA plan	Audit scope	Status	Findings			Overall report rating	Audit days per plan	Actual audit days
			High	Medium	Low			
	relation to the transition of income processing to the Integrated Clinic Portal.							
Information standards	Initially this review was to be aimed at providing assurance over the application of a new policy on the publication of patient oriented information on the HFEA's website. However, NHS England are assessing the information governance arrangements of the patient oriented information to ensure published information is up to date and accurate. Following a scoping meeting with the Audit Sponsor and to avoid duplication, it has therefore been agreed that our work should focus on the application of the policy to corporate information and information provided to clinics.	Scoping meeting held and date for review in January agreed.					5	0.25
Board effectiveness	This review has been a high level review to assess the Board effectiveness via a self-assessment survey and follow-up interviews.	Draft report issued	0	0	2	Not rated	6	6
Management of Cyber Penetration threat	Following scoping discussions with the Head of IT, it has been agreed that this work will be focussed on identifying security risks relating to a cloud environment and identifying any gaps in HFEA's security control framework.	Draft terms of reference issued. Fieldwork to be undertaken in December 2016.					5	0.75
Assurance	We will deliver an assurance mapping	Scope to be				Not	3	0

Reviews per 201/17 IA plan	Audit scope	Status	Findings			Overall report rating	Audit days per plan	Actual audit days
			High	Medium	Low			
mapping	workshop, having prepared a controls assessment framework for the area under review and agreed that with management. The area to be mapped will be agreed in consultation with management and the Audit and Governance Committee. There is the potential for this to be directed towards further considerations on Cyber Security, depending on the outcome of the initial work in that area as outlined above.	determined.				applicable – no rating will be provided as it is workshop		
Audit Management	All aspects of audit management to include: <ul style="list-style-type: none"> • Attendance at liaison meetings and HFEA Audit and Governance committees; • Drafting committee papers/progress reports; • Follow-up work; • Resourcing and risk management; and • Contingency. 	Ongoing	Not applicable			Not applicable	7	5
Contingency							5	-
Total Findings:			0	1	4			
						Total days	40	21

2.2 Summary of reports issued since the last Audit and Governance Committee:

Since the last Audit and Governance Committee in September 2016 we have issued the report on Board Effectiveness.

2.3 Follow-up work:

The HFEA performs its own follow-up work, reviewing the status of agreed audit actions and reporting progress to the Audit and Governance Committee.

As such, Internal Audit has been asked to provide independent assurance of the completion of agreed actions only over those actions which relate to high priority recommendations. This approach was agreed with the former Director of Finance and Resources.

No high priority actions have resulted from us undertaking the 2016/17 audit reviews to date and none were outstanding at the start of the year from previous audit work. Accordingly, there have been no outstanding high priority recommendations requiring internal audit follow-up work in the year to date.

2.4 Impact on Annual Governance Statement:

All reports issued with an overall Limited or Unsatisfactory rating, or with report findings that are individually rated high priority, should be considered for their possible impact on the Authority's Annual Governance Statement (AGS). To date, no Limited reports and no high priority issues have been raised as a result of us completing the work forming part of the 2016/17 audit plan and all actions relating to previous high priority issues have been completed. Accordingly, there are no matters arising from our work to date that we believe may require reference in the AGS.

Appendix 1 – Report Rating Definitions

Risk Ratings of individual findings:

Priority	Description
High	Fundamental weaknesses in control which expose the Accounting Officer / Director to high risk or significant loss or exposure in terms of failure to achieve key objectives, impropriety or fraud. Senior managers are expected to oversee the prompt implementation of agreed actions, or to confirm in writing that they accept the risks of not implementing a high priority internal audit recommendation.
Medium	Significant weaknesses in control, which, although not fundamental, expose the Accounting Officer / Director to a risk of loss, exposure or poor value for money. Managers are expected to oversee the prompt implementation of agreed actions, or to confirm in writing that they accept the risks of not implementing a medium priority internal audit recommendation. Failure to implement recommendations to mitigate these risks could result in the risk moving to the High category.
Low	Minor weakness in control which expose the Accounting Officer / Director to relatively low risk of loss or exposure. However, there is the opportunity to improve the control environment by complying with best practice. Suggestions made if adopted would mitigate the low level risks identified.

Ratings of audit reports

Substantial	In Internal Audit's opinion, the framework of governance, risk management and control is adequate and effective.
Moderate	In Internal Audit's opinion, some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	In Internal Audit's 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 Internal Audit's 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.

Appendix 2 - Limitations and responsibilities

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Future periods

Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or
- the degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems. We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected. Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.

Human Fertilisation and Embryology Authority

Audit planning report on the 2016-17 financial statement audit

REPORT TO THOSE CHARGED WITH GOVERNANCE
December 2016

<http://www.nao.org.uk/>

Contents

We have pleasure in setting out details of our proposed financial statement audit approach for the Human Fertilisation and Embryology Authority (HFEA) for the year ending 31 March 2017.

Financial statement audit plan	3
How are we going to conduct the audit – approach and team	4
When do we plan to complete this work – timetable and fee	5
Our audit approach	6
Significant financial statement risks	8
Risk factors and matters to keep in view	10
Follow up to recommendations we made in the previous year	11
Appendix 1: Fraud matters	12
Appendix 2: Future accounting standards	13
Appendix 3: Guidance on Governance	14
Appendix 4: Key messages from our wider work	15
Appendix 5: Quality assurance in NAO audits	17

We have prepared this report for HFEA's sole use although you may also share it with the Department of Health. You must not disclose it to any other third party, quote or refer to it, without our written consent and we assume no responsibility to any other person.

Financial statement audit plan

What work will we complete?

Our audit, which will be conducted in accordance with International Standards on Auditing (UK and Ireland) (ISAs (UK and Ireland)), will enable the C&AG to give an opinion on the financial statements.

Further details of the scope of the audit, as well as our respective responsibilities in relation to this engagement, have been set out in our Letter of Understanding issued on 23 October 2013 which has previously been separately provided to the audit committee.

Member of the Audit Committee are invited to consider and discuss:

- Whether our assessment of the risks of material misstatement to the financial statements is complete;
- Our proposed audit plan to address these risks; and
- Whether the financial statement could be materially misstated due to fraud, and communicate any areas of concern to management and the audit team.

How are we going to conduct the audit?

Risk based approach

We plan our audit of the financial statements to respond to the risks of material⁽¹⁾:

- misstatement to transactions and balances; and
- irregular transactions.

The auditing standards ISA 240 state that there is a significant risk in all entities for:

- Management override of controls to perpetrate fraud; and
- Presumed risk of fraud arising from revenue recognition.

Further details of these risks and our response are set out on pages 8-9.

In addition to these significant risks we have also identified one 'risk factor' i.e. a risk that is not expected to represent a material misstatement in the year but we would like to keep in view in our audit work (details on page 10):

- HFEA's judicial review case

Our team

The details of the key audit staff who will complete this audit are:

- George Smiles, Engagement Director
- Sarah Edwards, Engagement Manager
- Payal Patel, Engagement Lead for audit and will complete the on-site work.

^[1] A matter is material if its omission or misstatement would reasonably influence the decisions of users of the financial statements. The assessment of what is material is a matter of the auditor's professional judgement and includes consideration of both the amount and the nature of the misstatement. Further information on materiality is included on page 6.

When do we plan to complete this work?

Timetable

The timetable comprises an interim visit week commencing 23 January 2017 for 1 week and a further second interim visit week commencing 13 March 2017 for 1 week and a final visit commencing 30 May 2015 for 2 weeks with certification planned for start of July 2017. Further details are provided in the table below.

Date	Activity
September/October 2016	Planning: review HFEA's operations, assess risk for our audit and evaluate the control framework.
January 2017	Interim audit work: test expenditure and income.
February 2017	Update to audit committee on interim work.
30 May 2017	Receipt of 1st draft account
May 2017	Final audit work: test expenditure and income and significant balances and disclosures.
June 2017	ISA 240 report including management letter: compromising audit completion report and management letter to be presented to the audit committee.
July 2017	Certification: seek representations and C&AG issues opinion.

Fees

The fee for the audit is £28,000 (PY £27,500).

Completion of our audit in line with the timetable and fee is dependent upon HFEA:

- delivering a complete Annual Report and Accounts of sufficient quality, subject to appropriate internal review on the date agreed;
- delivering good quality supporting evidence and explanations within the agreed timetable;
- making staff available during the audit.

If significant issues arise and we are required to perform additional work this may result in a change in our fee. We will discuss this with you before carrying out additional work.

Our audit approach

Our assessment of materiality

Materiality

The concept of materiality recognises that financial statements are rarely absolutely correct, and that an audit is designed to provide reasonable, rather than absolute, assurance that the financial statements are free from material misstatement or irregularity.

For the purposes of determining whether the financial statements are free from material misstatement or irregularity we consider whether:

1. the magnitude of misstatement; or
2. the nature and cause of misstatements (e.g. because of the sensitivity of specific disclosure or regularity requirements)

would influence the users of the accounts.

In line with generally accepted practice, we have set our quantitative materiality threshold based on our judgement of a range of factors including historic error and level of expenditure.

Other elements of the financial statements that we consider to be more sensitive to users of the accounts will be assessed using a lower qualitative materiality threshold. These elements include the remuneration report disclosures; the losses and special payments note; our audit fee.

We apply the concept of materiality in planning and performing our audit and in evaluating the effect of misstatements on our audit and on the financial statements. As the audit progresses our assessment of both quantitative and qualitative materiality may change.

Error reporting threshold

For reporting purposes, we will treat any misstatements below £2,500 as “trivial” and therefore not requiring consideration by the Audit Committee.

Please note that this is a separate threshold to our consideration of materiality as described above. It is materiality, not the error reporting threshold, which is used in forming our audit opinion.

Our audit approach

Other matters

Independence We comply with relevant ethical requirements regarding independence and have developed important safeguards and procedures in order to ensure our independence and objectivity.

Information on NAO quality standards and independence can be found on the NAO website: <http://www.nao.org.uk/about-us/role-2/what-we-do/audit-quality/audit-quality/>

We will reconfirm our independence and objectivity to the Audit Committee following the completion of the audit.

Management of personal data

During the course of our audit we have access to personal data to support our audit testing.

We have established processes to hold this data securely within encrypted files and to destroy it where relevant at the conclusion of our audit. We confirm that we have discharged those responsibilities communicated to you in the NAO's Statement on Management of Personal Data at the NAO.

The statement on the Management of Personal Data is available on the NAO website: <http://www.nao.org.uk/freedom-of-information/publication-scheme/how-we-make-decisions/our-policies-and-procedures/policies-and-procedures-for-conducting-our-business/>

Using the work of internal audit

We liaise closely with internal audit through the audit process and seek to take assurance from their work where their objectives cover areas of joint interest.

Following our review of internal audit's plans we will consider the outcome of the planned report for the Information for Quality capital expenditure project.

Significant financial statement risks (1)

Management override of controls (ISA 240)



Key features

- Under International Standards on Auditing (UK and Ireland) 240 The Auditor's responsibilities relating to fraud in audit of financial statements there is a presumed risk of management override of controls in all organisations, We are required to assess the risk of material misstatements arising from management override, in particular in relation to significant or unusual transactions, bias in accounting estimates and journals.

Change from prior year

Same approach to meet ISA 240 requirements

Audit response

Substantive

- Review of significant transactions;
- Journal sample testing
- Consider the assumptions underpinning each of the key estimates in the accounts (i.e. provisions and impairments).

Significant financial statement risks (2)

Revenue Recognition

Key features

- Under International Standards on Auditing (UK and Ireland) 240 The Auditor's responsibilities relating to fraud in audit of financial statements there is a presumed risk of fraud in revenue recognition, albeit rebuttable in all entities. As HFEA's main income stream is treatment fees from clinics; there is a risk that not all treatment income is reported to HFEA.

Change from prior year

Same approach to meet ISA 240 requirements

Audit response

Substantive and controls testing

- A substantive analytical procedure will be performed by using the invoices sent to clinics.
- We will be assessing the work that the Compliance Audit team carry out on their visits to clinics. This is the control we will seek to rely for income, in order to provide us with assurance that the data provided by the clinics to HFEA is complete and accurate.

Risk factors

Risk factors represent developments or ongoing issues in HFEA that are potential risks to the financial statements or the C&AG's audit opinion. They differ from significant risks as they do not currently require a specific audit response other than already covered by our standard audit approach.

HFEA's judicial review case

HFEA is subject to a judicial review relating to the IfQ project. A risk exists, depending on the outcome of the JR that the IfQ project may be delayed which could increase costs relating to this project and , more widely, may damage HFEA's reputation. We await the outcome of the JR.

Other Matters

These are issues that we do not anticipate giving rise to a risk to the financial statements or the C&AG's opinion but may have an impact on HFEA.

Information for Quality expenditure

HFEA need to ensure that any expenditure relating to IfQ that is capitalised in year meets the recognition criteria as set out on IAS 38 intangible assets.

New Finance Director

The new FD has recently taken up post and, as with any change of personnel at a senior level, there is a loss of corporate knowledge particularly when a long-standing member of staff leaves. We will consider the actions that HFEA takes to ensure that there is no consequential adverse impact on the operation of the overall controls environment following this change in personnel.

Brexit

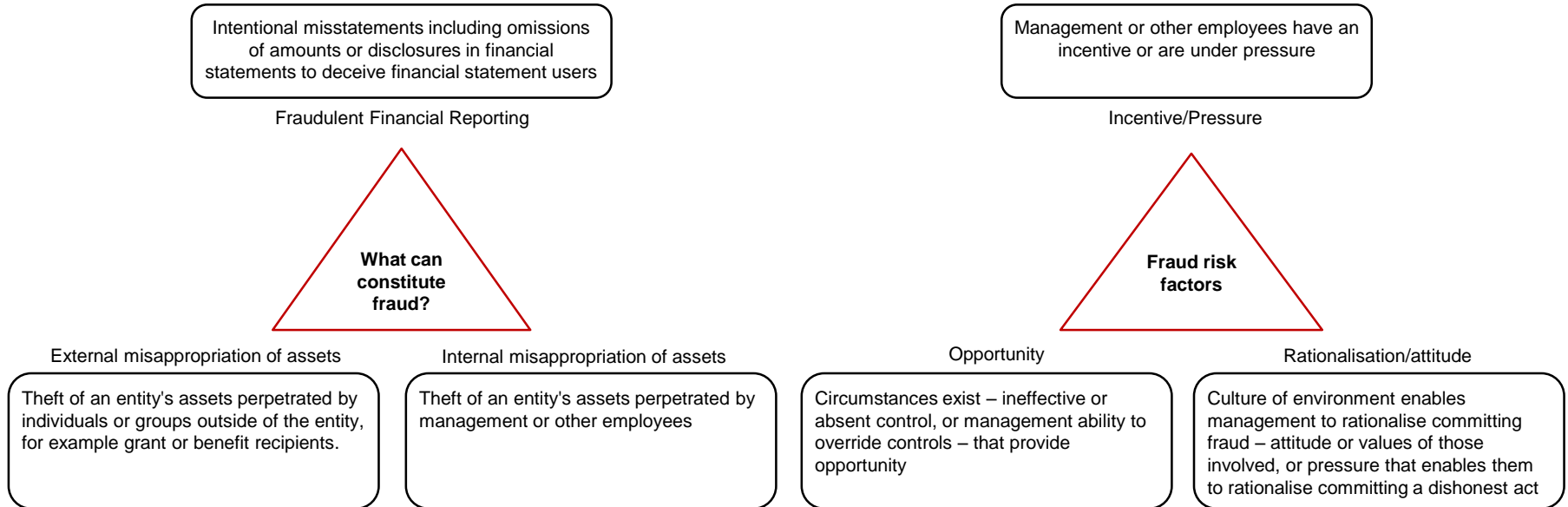
All EU laws to be transposed into UK law, and so we do not expect this to affect our audit. However due to the recent announcement on timing that Article 50 is to be triggered in March 2017, management will need to consider any impacts on the Financial Statements and disclosures after March 2017.

Follow up to recommendations we made in the previous year

Title	Area	What was the recommendation?	Response/Progress	Status
Capitalisation of expenditure	Intangible Assets	Management need to ensure they only capitalise what is permitted under Accounting Standards IAS 38. This consideration should be ongoing, for instance the treatment of maintenance/ enhancement of systems,	HFEA are in the process of conducting a piece of work on the IfQ expenditure and hope that this will be completed by the time the NAO attend for their interim visit.	Ongoing

Appendix 1 - Fraud matters

ISA 240 (UK&I) 'The auditor's responsibility to consider fraud in an audit of financial statements' requires us, as your auditors, to make inquiries and obtain an understanding of the oversight exercised by those charged with governance.



ISA inquiries

Our inquiries relate to your oversight responsibility for:

- Management's assessment of the risk that the financial statements may be materially misstated owing to fraud, including the nature, extent and frequency of such assessments;
- Management's process for identifying and responding to the risks of fraud, including any specific risks of fraud that management has identified or that has been brought to its attention;
- Management's communication to the Audit Committee (and others charged with governance) on its processes for identifying and responding to the risks of fraud; and
- Management's communication, if any, to its employees on its views about business practices and ethical behaviour.

We are also required to ask whether you have any knowledge of any actual, suspected or alleged fraud.

Audit approach

We have planned our audit of the financial statements so that we have a reasonable expectation of identifying material misstatements and irregularity (including those resulting from fraud). Our audit, however, should not be relied upon to identify all misstatements or irregularities. The primary responsibility for preventing and detecting fraud rests with management.

We will incorporate an element of unpredictability as part of our approach to address fraud risk. This could include, for example, completing procedures at locations which have not previously been subject to audit or adjusting the timing of some procedures.

We will report to the Assurance and Risk Committee where we have identified fraud, obtained any information that indicates a fraud may exist or where we consider there to be any other matters related to fraud that should be discussed with those charged with governance.

Appendix 2: Future accounting standards (not specifically relevant to HFEA, for information only)

IFRS 9: *Financial instruments*

Effective from 2018-19

[IASB project summary](#)

Replacing IAS 39, IFRS 9 aims to simplify financial instrument accounting and more closely align accounting and practices with how instruments are used in the business. Specifically:

- **classification and measurement** rules have been adapted to incorporate a more principles-based model with fewer categories – with measurement at fair value except for some debt instruments depending on characteristics;
- **impairments** due to changes in credit quality will result in earlier remeasurement, on an ‘expected loss’ basis; and
- **hedge accounting** will become more principles-based, with the elimination of the 80-125% effectiveness test and a greater reliance on assessing the purpose of transactions within businesses’ risk management strategies.

IFRS 15: *Revenue from Contracts with Customers*

Effective from 2018-19

[IASB project summary](#)

IFRS 15 aims to replace a significant amount of existing guidance and reduce inconsistencies by setting a new principles-based Standard.

The step by step process in IFRS 15 involves identifying contractual performance obligations, allocating the transaction price to those obligations, and recognising revenue only when those obligations are satisfied. Impact for most central government clients will be limited.

IFRS 16: *Leases*

Effective from 2019-20

[IASB project summary](#)

[2013 exposure draft](#) (now superseded by issued Standard)

Decisions remain for HM Treasury on if or how to interpret/adapt this Standard for FReM bodies, and what allowances to make for transitional relief.

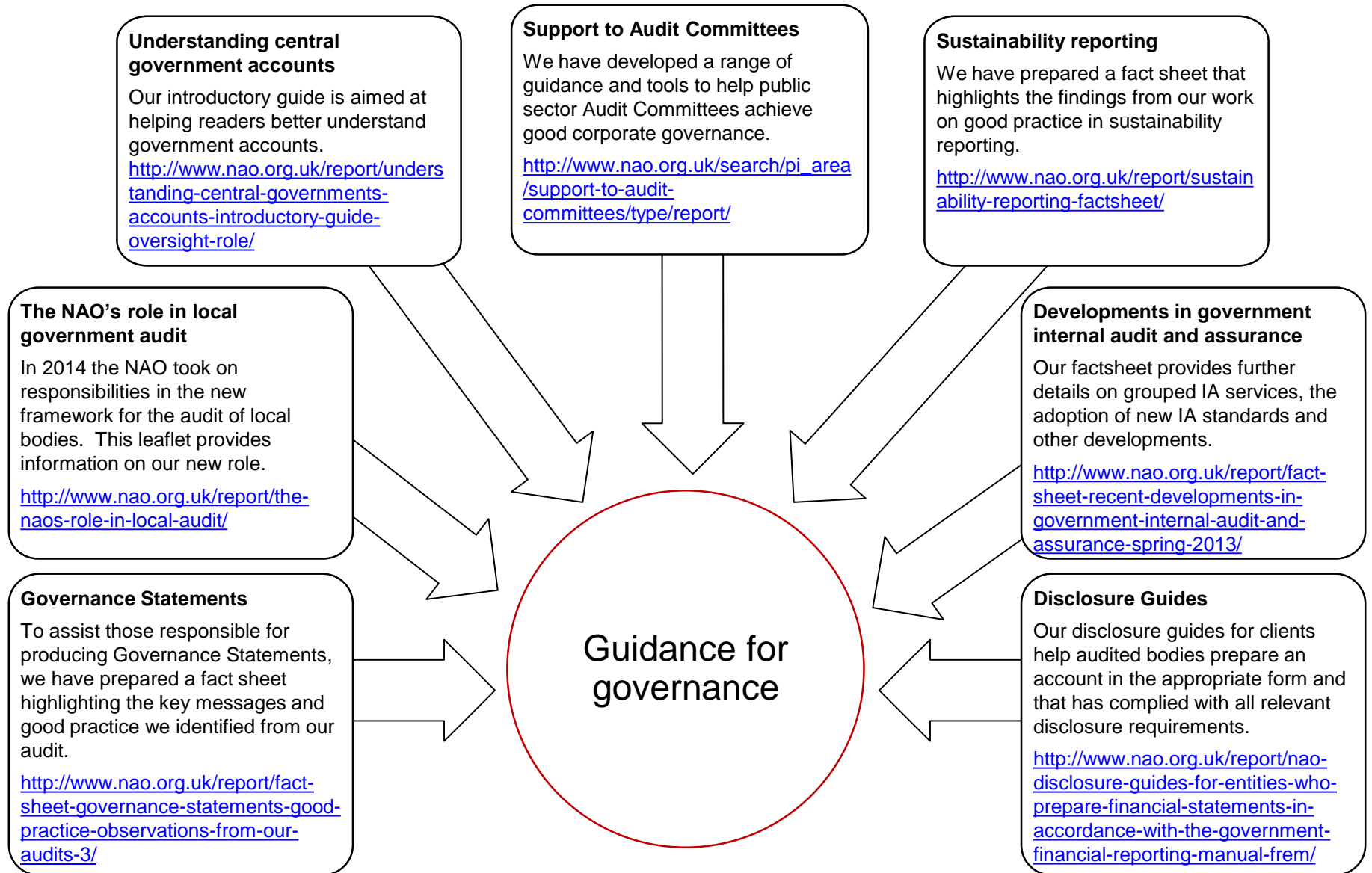
IFRS 16 eliminates the operating/finance lease distinction and imposes a single model geared towards the recognition of all but low-value or short term (<12m) leases. The proposals arise partly from the IASB’s view that:

- disclosures around operating lease commitments have lacked prominence and tended towards understatement; and
- even in leases where the underlying asset is not acquired for its whole useful life, the lessee nevertheless acquires an economic right to its use, along with obligations to make good on minimum lease payments.

These will now be recognised on the Balance Sheet as a ‘**right of use**’ asset and **lease liability**. The lease liability will be measured at initial recognition as the value of future lease payments, with the asset additionally including any initial direct costs incurred by the lessee, plus an estimate of any dismantling/restoration costs. Subsequent measurement of both asset and liability will need to respond to any changes in lease terms, and the accounting for the asset can be on a *cost less depreciation and impairment* model or a *revaluation* (fair value) model.

Successful transition will depend on organisations pro-actively capturing additional information about leases – new and existing – which they expect to remain in place at 1 April 2019, especially regarding future minimum lease payments. Organisations should also ensure systems for capturing cost information are fit for purpose, can respond to changes in lease terms and the presence of any variable (e.g. RPI-based) lease terms where forecasts will need to be updated annually based on prevailing indices.

Appendix 3: Guidance for Governance (not all relevant for HFEA)



Appendix 4 - Key messages from our wider work

	<p>The UK government detected fraud figure of 0.02% of expenditure is significantly lower than some estimates of 3-5% in the EU and US. While comparisons should be treated with caution, this suggests there could be significant fraud and error which is unreported or undetected and losses which are not being adequately addressed.</p>
Cross Government Fraud Landscape Review	<p>Concludes that, overall, the Government lacks a clear understanding of the scale of the fraud problem and departments vary in their ability to identify and address fraud risks. The data that does exist is patchy, inconsistent and of variable quality. The most comprehensive data relates to areas of known risk – tax credit and benefit fraud – but information across the rest of government is clearly incomplete. It is difficult to formulate solutions if the scale and nature of the problem is unknown.</p>
(February 2016)	<p>www.nao.org.uk/report/fraud-landscape-review</p>

	<p>NHS England's spending on the 146 specialised services it offers has increased at a much greater rate than other parts of the NHS. There is no overarching service strategy and increasing demand for effective but expensive new drugs is adding to existing financial pressures. Governance arrangements for specialised commissioning are ineffective and there are concerns over the transparency of decision making.</p>
The Commissioning of Specialised Services in the NHS	<p>Concludes that if NHS England is unable to control spending on specialised services this will affect its ability to resource other services, such as primary care. Without consistent information from all providers on costs, access to services and outcomes, it cannot manage the ongoing pressure on its budget for specialised services, make effective strategic decisions or gain assurance that its objectives are being met.</p>
(April 2016)	<p>www.nao.org.uk/report/the-commissioning-of-specialised-services-in-the-nhs</p>

Appendix 4 - Key messages from our wider work

Departments’ oversight of arm’s- length bodies: a comparative study

(July 2016)

We looked at and compared how four departments oversee and manage the relationships with their arm’s-length bodies (ALBs). These departments are BIS (now BEIS), MoJ, Defra and DCMS.

There is no single list of ALBs across government nor a common understanding of when ALBs should be used or what type of ALB is most appropriate for particular circumstances. Although the Cabinet Office is building on its Public Bodies Reform Programme and taking further steps to address these shortfalls, the prevailing inconsistency hampers a coherent approach to overseeing ALBs that is consistent with their purpose.

To get the best from ALBs we recommend the Cabinet Office works with departments to improve understanding of the costs and benefits of different approaches, and develop and implement a guiding framework for effective oversight. We propose a principles-based approach. We do not argue for a one size fits all approach, but it’s clear that the broad range of approaches cannot all be equally good at getting value from ALBs.

www.nao.org.uk/report/departments-oversight-of-arms-length-bodies-a-comparative-study

Protecting information across government

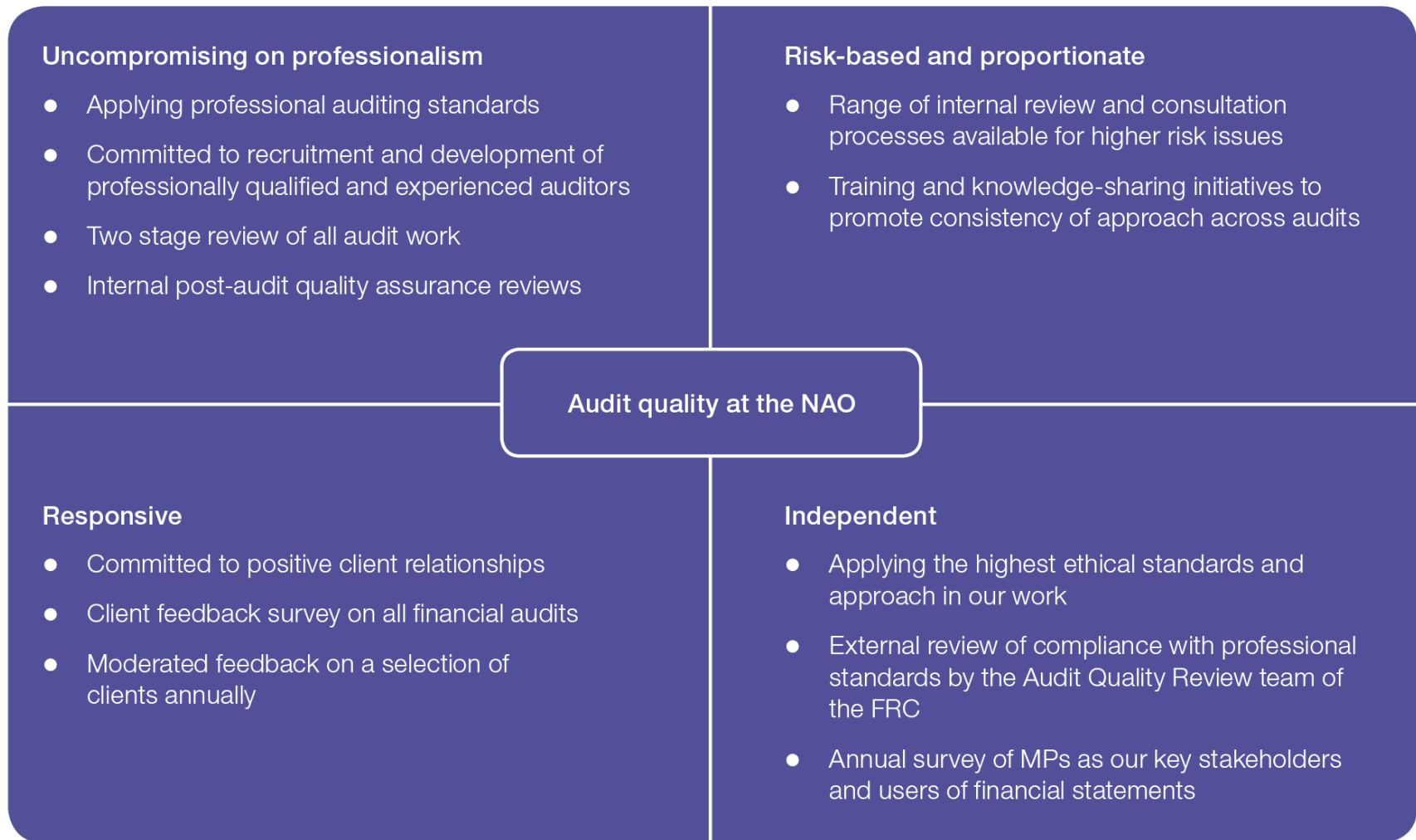
(September 2016)

Protecting information while re-designing public services and introducing new technology to support them is a complex challenge for government. The responsibility for protecting information held by government from unauthorised access or loss must increasingly be balanced with the need to make information available to other organisations, users and citizens via new digital services.

We considered the effectiveness of government in managing the risk of information loss, including cost, breach reporting and deployment of the right skills. We found that some departments have made significant improvements in information governance, but most have not given it the same attention as other forms of governance. We also found that few departments have the skills and expertise to risk manage their information by themselves and will continue to depend on effective support from the centre of government. But at present too many bodies, with overlapping responsibilities, operate in the centre of government, confusing departments about where to go for advice. Although the new National Cyber Security Centre (NCSC) will bring together much of government’s cyber expertise, wider reforms will be necessary to further enhance the protection of information.

www.nao.org.uk/report/protecting-information-across-government/

Appendix 5: Quality assurance in NAO audits



Implementation of Audit Recommendations – Progress Report

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

Details:

Meeting	Audit and Governance Committee
Agenda item	10
Paper number	[AGC (07/12/2016) 518 WEC]
Meeting date	7 December 2016
Author	Wilhelmina Crown - Finance & Accounting Manager

Output:

For information or decision?	Decision
Recommendation	AGC is requested to review the enclosed progress updates and to comment as appropriate.
Resource implications	As noted in the enclosed summary of outstanding audit recommendations
Implementation date	As noted in the enclosed summary of outstanding audit recommendations
Organisational risk	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High

Report

- 1.1. This report presents an update to the verbal briefing given to this committee at its meeting in September 2016.
- 1.2. These recommendations were received and agreed for follow up action by this committee in September.
- 1.3. Recommendations are classified as high (red), medium (amber) or low (green).
- 1.4. Three new recommendations were received with one noted as medium and two as low.
- 1.5. Recent updates received from Action Managers are recorded under a November 2016 heading in this document.
- 1.6. Two recommendations are noted as completed with one due to be completed by end December 2016.

Recommendation

AGC is requested to review the enclosed summary of recommendations and updated management responses and to advise whether they have any comments or queries in respect of them.

Annex 1: Summary of Recommendations

Recommendation Source	Status / Actions	2015/16	Total
Internal – <i>DH Internal Audit</i>	<i>Complete</i>	2	2
	<i>To complete</i>	1	1
COUNT		3	3

FINDING/RISK	Recommendation	Agreed actions / Progress Made	Owner/Completion date
2015/16 – INTERNAL AUDIT CYCLE			
INCOME GENERATION			
1. Follow-up procedures with those clinics that do not submit activity data could be more robust.			
<p>Clinics that have not submitted data to the HFEA for a period longer than one month are identified by the Head of Information and the Senior Network Analyst on a monthly basis. However, this is primarily to allow accurate accruals and deferrals of income to be made rather than to enable HFEA to identify clinics that may be having issues in submitting data. Some follow up is performed if a particular issue is noted, but this is on an ad hoc basis and there is no formalised process to follow-up all clinics to identify whether data should have been received.</p>	<p>The monthly report of clinics which have not submitted data for one month should be used as a basis to ensure that clinics have been, or are, contacted or otherwise checked to identify the reasons and any action that HFEA may need to take to resolve any issues.</p> <p>The reasons for any problems that clinics are experiencing should be documented and progress monitored. The record could be cross referenced to the IT support system ticket number(s) where the cause is an IT matter</p>	<p>Using the monthly report of clinics which have not submitted data for a month, a document will be created listing the clinics and the problems they are experiencing, the person responsible for resolving the issue and the status of the problem. This will be discussed in a monthly meeting with actions designated to appropriate individuals to resolve them and to contact the clinic as necessary.</p> <p><u>November 2016 update:</u> Check has already been done for November. The appropriate Register SOP will be updated prior to December's, to enable monthly checking.</p>	<p>Head of Information</p> <p>Date: September 2016 billing run</p> <p>End December 16</p>
2. Review of the error report which identifies missing invoices is only performed quarterly and no evidence of this review is maintained.			
<p>It is our understanding that the Finance Manager generates an error report ("uspReport_ABSMissingInvoiceImages) on a quarterly basis to identify any missing invoices. However, this process is not evidenced. In addition, we suggest consideration be given to whether this control might more effectively be performed on a monthly basis so any omissions can be identified on a more timely basis.</p>	<p>Whilst we recognise that the last issue to be identified from the report was in February 2014, we suggest that consideration be given to generating and reviewing the report on a monthly basis to ensure that any missing invoices are identified in a timely manner.</p> <p>Evidence of the review should also be retained.</p>	<p>The exception report will be run on a monthly basis and the evidence retained.</p> <p><u>November 2016 update</u></p> <p>The action has been implemented and the exception report now forms part of the monthly billing process.</p> <p><u>Recommendation Complete</u></p>	<p>Finance & Accounting Manager</p> <p>Date: August 2016 billing run</p> <p>COMPLETE</p>

3.

Action plans in response to the risks associated with transition of the billing process to the new Integrated Clinic Portal have yet to be identified.

Risks relating to the Information for Quality (IfQ) programme are being identified and captured in a Risk Log, with specific owners, action plans and timelines, and the risks are discussed monthly during the IfQ programme board meetings. At the time we started our review, no risks specifically relating to the transition of the income process had been included within the log, but the Head of Information did add them during the course of our review. As with other risks, they were then due to be discussed at the next monthly board meeting where relevant action plans should be identified. Consequently, at the time of our review there were no plans in place to respond to these specific risks and while there is a formal process to ensure that this is addressed it is important that this is completed promptly to ensure actions are in place in good time to mitigate the risks that HFEA faces.

Whilst we recognise that there is a formal process in operation to ensure that risks are responded to and that the new Integrated Clinic Portal is not due to be implemented until the end of October, management should ensure that appropriate action plans are identified and implemented on a timely basis.

Action plans addressing the risks relating to the transition of the income process will be identified during the next board meeting.

[November 2016 update](#)

An options paper has been presented to and considered by the IfQ Programme Board and Senior Management Team.

[Recommendation Complete](#)

Head of Information

Date:
September 16
board meeting

COMPLETE

Cyber Security - Information Security & Testing

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

Details:

Meeting	AGC
Agenda item	11
Paper number	[AGC (07/12/2016) 519 DM]
Meeting date	07 December 2016
Author	David Moysen, Head of IT

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	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input checked="" type="checkbox"/> High

Annexes

Annex A - Application Security assessment
Annex B – IfQ security model

1. Introduction and summary

- 1.1. The purpose of this report is to provide the Committee with our approach to cyber security, further to its request following an oral presentation at its last meeting.

2. Background

- 2.1. The National Cyber Security Strategy 2016-2021 was published in November 2016 and noted the UK is critically dependent on the Internet. 'However, it is inherently insecure and there will always be attempts to exploit weaknesses to launch cyber attacks. This threat cannot be eliminated completely, but the risk can be greatly reduced to a level that allows society to continue to prosper, and benefit from the huge opportunities that digital technology brings.
- 2.2. Our systems have grown and developed over the years alongside the growth of cyber threat. We have put in place a range of mechanisms, and ways of providing assurance, that those mechanisms are effective, to guard against threat.
- 2.3. At the last meeting of the Audit and Governance Committee an oral presentation set out the steps the HFEA is taking, as the IFQ programme moves from development to implementation, to ensure cyber security. This paper builds on that presentation and provides documentation supporting our assessment that, in developing our new systems within the Information for Quality Programme, our arrangements are as secure as possible.

3. Standards

- 3.1. There is a plethora of standards, assurance frameworks and expectations in place. The '10 Steps to Cyber Security' are widely known and are recognised as an effective means of raising awareness of cyber threats within the leadership of organisations, and to enable a greater capability to safeguard their most important information assets, such as personal data, online services and intellectual property. The 10 Steps to Cyber Security features controls to reduce risks in the following areas:
- Information Risk Management Regime;
 - Secure Configuration;
 - Network Security;
 - Managing User Privileges;
 - User Education and Awareness;
 - Incident Management;
 - Malware Prevention;
 - Monitoring;
 - Removable Media Controls;
 - Home and Mobile Working.
- 3.2. The HFEA has a successful track record in ensuring its systems, over time, meet these important expectations. We have policies in place relating to information governance and security. Periodically, we have sought assurance by a range of means including review by internal audit and penetration testing (carried out by independent third party experts) and by the application of regular vulnerability assessments.

- 3.3.** Equally the HFEA has devoted two years to a fundamental redesign of its information architecture. Principles relating to security considerations have been built in from inception.
- 3.4.** The IFQ team has adopted the principle of “Secure by Design”. This is an approach, developed in conjunction with our retained security consultant working alongside us since the inception of the Programme, which has as its paradigm that software and systems are designed and implemented with security in mind from the ground up.
- 3.5.** The HFEA is developing an Assurance Plan leading to a full Risk Management and Accreditation Document Set for approval prior to the EDI replacement going live. This RMADS is being developed by an independent security consultant. In effect, this document provides details about the system being developed and a full risk assessment. The document will then go on to provide details of how risks are to be mitigated by the application of a Baseline Control Set and will need to be signed off by the Siro prior to the application going live. Current CESG guidance suggests that the RMADS approach is often disproportionate in terms of the effort that is required and that the business should decide what level of risk management is suitable to its needs. However, given the sensitive nature of the data the HFEA feels that the creation of an RMADS is proportionate.

4. Security progress to date

- 4.1.** The high level aims of the security objectives are set out here, and ensure the:
 - i. Confidentiality, integrity and availability of the sensitive data held in the solution
 - ii. Confidentiality, integrity and availability of all data and systems in all environments hosting the systems. (This includes stages of development, testing, pre-production and production).
 - iii. Solution adheres to relevant legislation and regulatory standards
 - iv. Solution (and any infrastructure changes required for it) do not have any effect on the operations of the core corporate systems.
 - v. Reputation of the organisation is not damaged by any activities surrounding the implementation and operation of the new systems.
- 4.2.** A set of technical security model documents have been produced as part of the Programme – principally for use by the various internal and external development teams to ensure integrity with the model and to provide background briefing information to independent assessors, contracted to provide external assurance.
- 4.3.** Appendix A contains the IfQ security model and high level security and architecture solutions for the HFEA Clinic Portal and the Release 2 data submission (EDI) replacement systems. Whilst these are dense and technical in nature given the audience they are intended for they are a demonstration that the architecture is being developed with security at its core, and are annexed as information.
- 4.4.** Nevertheless, what is more important is that there is a programme of independent assessment for vulnerabilities in place, providing assurance to the SIRO, Authority and the Audit and Governance Committee.

- 4.5.** Members are aware there are three main components of the Programme – the HFEA website; the HFEA Clinic Portal; and ‘Release 2’ of the Clinic Portal – the ability for clinics to submit treatment information to the HFEA. (A separate agenda item updates the Committee on progress with the IfQ Programme more generally). In terms of security, the website is lowest risk; increasing with the Portal (as there is more two-way interaction) and reaches its peak with Release 2. Currently, the system threat is limited as there is a direct link between clinics and the HFEA. The new system is browser based and therefore the ‘attack surface’ is greatly increased.
- 4.6.** Our testing programme is established in two phases – firstly at Beta (broadly) and then prior to live release. The HFEA website and Clinic Portal have been independently assessed for vulnerabilities at the Beta stage, with the recommendations made in the report addressed. It reported:
- 4.7.** “In general, the security of the application components reviewed was high, as the applications are employing some of the latest technologies from Microsoft they are following good security practices in the main when it comes to the application code with no apparent weaknesses that are covered by the OWASP Top 10, such as Cross Site-Scripting and Injection attacks being handled by the .NET platform security features. The application is employing security features of the platform to provide protection as a
- 4.8.** result when testing many types of attack are being defended by these features as a result it is not possible to fully assess the underlying code for weaknesses should the platform protect fail or be removed.”
- 4.9.** The full report produced by Reaper Technologies is at annex B.
- 4.10.** We have now engaged a CESG Check approved consultancy who will be performing end to end vulnerability assessment of the HFEA website, Clinic Portal and Release 2 in addition to penetration testing of the HFEA’s perimeter network as each aspect of the Programme goes live. The IfQ Programme Board receives these reports, and further updates will be provided to the Audit and Governance Committee as part of the update reports by the Director of Compliance and Information.
-

5. Recommendation:

- 5.1.** The Audit and Governance Committee is asked to:
- Note this report
-

6. Annexes:

- Annex A - Application Security assessment
- Annex B – IfQ security model

Annex B
Audit and Governance Committee 7 December 2016
Agenda item 11 - Cyber Security



APPLICATION SECURITY ASSESSMENT
FOR
HUMAN FERTILISATION AND EMBRYOLOGY AUTHORITY

Security Assessment Summary
28 May 2016



Client Information

Company Name:	Human Fertilisation and Embryology Authority
City:	10 Spring Gardens London SW1A 2BU
URL:	http://www.hfea.gov.uk

Client Contact Information

Contact Name:	David Moysen
Title:	Head of IT
E-mail:	David.Moysen@hfea.gov.uk

Consultant Information

Company Name:	Reaper Technologies Limited
Contact Name:	Stephen Kapp
Telephone:	+447770566687
E-mail:	skapp@reapertech.com

1.0 Business Risk Summary

Overview

A security review was conducted of the new HFEA website, portal and supporting API. The review looked at assessing the services against the OWASP Top 10 to determine if any security issues were present. The following is a summary of the findings and conclusions and recommendations based on these findings.

The security review was conducted between the 10th and 24th May (5 days) and looked at the following services:

- ifq-website.azurenetworks.net
- ifq-portal.azurenetworks.net
- ifqclouddevwebapi.azurewebsites.net

General

In general, the security of the reviewed applications was good, the website and portal leverage the Umbraco CMS platform to provide the frontend elements, with extensions implemented to provide specific features for the HFEA. The Umbraco CMS platform is a web supported .NET based CMS and HFEA appear to be running the latest release. The entire frontend is hosted on Microsoft Azure and uses various elements of the Azure platform to provide services for the application, for example authentication is provided through integration with the authentication services provided by the Azure platform.

During the course of the assessment each of the areas was tested for common security vulnerabilities including those outlined in the OWASP Top 10 the review did not identify any significant issues, however there are some areas of concern as detailed as follows.

Communications Security

The first area of concern was the security of the communications with the HFEA systems, neither the website or the portal required the use of TLS to provide transport security to the application. As a result authentication information for the portal and authentication information for the management of the Umbraco CMS is not protected as it is transmitted over the Internet.

As a result, the lack of transport security means that features such as Strict Transport Security and protection mechanisms for preventing eavesdropping of session cookies are not present.

The backend API however was protected by HTTPS; this was using the default SSL termination for the azurewebsites.net domain.

It is recommended that all externally visible components of the application are secured by using HTTPS to ensure that all information is protected while in transit, with requests to the HTTP version of the applications redirected to the secured versions. Additionally, once this has been implemented implement Strict Transport Security and options on session cookies to further secure the information transmitted.

Information Leakage through Error Messages

During the course of the security assessment a number of error messages were recorded that leaked potentially useful information regarding the environment the application runs within. The error messages in themselves did not leak anything sensitive in terms of the data handled by the applications, however they did leak system information for example one error message leaked the path information for the application on the server and detailed call stack information. This type of information is useful for an attacker, it can provide them useful insight into the application, providing the attacker with a location for files on the system as well as being able to deduce the version of the Umbraco CMS in use.

Information like this can be used to improve the success of other attacks or provide enticement information for areas to exploit. As a result it is highly recommended that custom error handling is implemented to capture errors, log the specifics of the errors to a log file for investigation and return a basic minimal error response to the application user.

Umbraco CMS Configuration

There is an concern within the Umbraco CMS environment, some default content appeared exist without having been removed or default configuration changed. This doesn't follow best practice as recommended by the Umbraco maintainers. It could be

indicative of other elements of the Umbraco code that may not have been properly configured to remove default settings or features.

It is recommended that the Umbraco installation 'hardening' be completed. Ensure that default configurations have been customised and unused features are disabled or removed from the environment.

Conclusions and Recommendations

In general, the security of the application components reviewed was high, as the applications are employing some of the latest technologies from Microsoft they are following good security practices in the main when it comes to the application code with no apparent weaknesses that are covered by the OWASP Top 10, such as Cross Site-Scripting and Injection attacks being handled by the .NET platform security features. The application is employing security features of the platform to provide protection as a result when testing many types of attack are being defended by these features as a result it is not possible to fully assess the underlying code for weaknesses should the platform protect fail or be removed.

It is recommended that the application code undergo a security review to provide insight into the security of the application code at a deeper level. This would be in the form of a source code review and it is also recommended that as part of the build and deployment process a static code analysis step be introduced to provide insight into code issues as the application is being developed with any identified problems being fed back into the development teams to be addressed earlier in the development process.







As the application development progresses with the next phases where patient data being handled it is more important that the security of the application code is reviewed in more depth. Any source code review would look for the common security weaknesses, static analysis tools will help identify these, however another area that would be reviewed by a manual review would be the logic behind the scenes to assess if there are any issues being introduced.

Additionally, to help going forward with the identification of potential areas of concern and to guide remediation and development of security controls and features I would recommend that the next phase of development have a Threat Modelling exercise performed. This threat model would then be used to guide the future design and implementation to ensure that later phases of development address security risks.

2.0 Technical Summary

2.1 Test Area Summary

The following is a summary of the posture of the applications reviewed as part of this assessment.

Vulnerability Area	Brief Description	N/A	Good	Fair	Weak	Poor
Configuration	How secure the configuration of the application is.					
Authentication	Are there any specific issues regarding the authentication of users.					
Session Management and Authorisation	How well the application handles the authorisation and keeps the session secure.					
Encryption	Is there any encryption in place in the application and how well it is configured.					
Data Validation	How well the application handles sensitive user input.					
Error Handling	How the application reacts when an error occurs					

2.2 Test Findings

The assessment findings are included in the accompanying spreadsheet.

3.0 Risk Rating

This report harnesses the power of CVSS v3, the latest industry standard for vulnerability scoring, it combines this with the simplicity of colour coding. This enables access to this report by all levels of management.

CVSS v3 Explanation

CVSS (currently version 3) is the Common Vulnerability Scoring System. This is a vendor independent way of scoring vulnerabilities in a more granular way than just being assigned as a critical, high, medium, low or no (informational) risk.

This system takes a variety of factors (known as metrics) into account such as the level of complexity required to reach the affected system, whether or not exploit code exists, the impact successful exploitation of the issue would have on the business and the type of area of concern (availability, confidentiality and integrity).

By applying these factors to each unique vulnerability, a score from 0 to 10 calculated and assigned.

Reaper Technologies assigns high, medium or low to each vulnerability based on the following criteria as defined by the CVSS v3 standard:

Critical:	Any issue with a CVSS score of 9.0 or higher
High:	Any issue with a CVSS score of 7.0 or higher but lower than 9.0
Medium:	Any issue with a CVSS score of 4.0 or higher but lower than 7.0
Low:	Any issue with a CVSS score of 0.01 or higher but lower than 4.0
Informational:	Any issue with a CVSS score of 0.0

This assures that each vulnerability has been tailored to the client, as each vulnerability affects each client in different ways.

For example, an SQL injection issue affecting a public facing website would be an high risk. That same issue on an internal host with adequate firewall configurations could be classed as a medium risk. A high risk issue on a low impact server may carry a lower CVSS score than a medium risk issue on a critical server.

For more information on CVSS please refer to the First.org website link below: <http://www.first.org/cvss/>

IFQ Security Model

Identity Solution

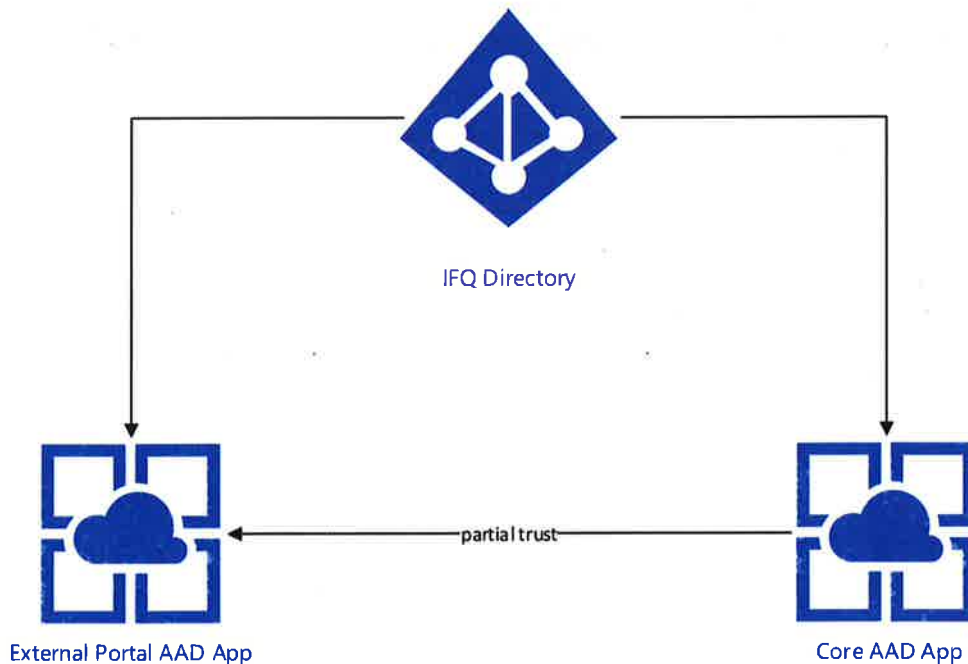
We have chosen Azure Active Directory (AAD) to store user identities. AAD replicates well both with Microsoft Active Directory and third party providers. In addition to that AAD supports modern identity standards such as OpenID Connect and OAuth 2.0, as well as multi factor authentication when required in future.

Azure Active Directory Partitioning

IFQ Application owns a separate directory in HFEA Azure Tenant. That means it's totally separate from any other directories in the Azure Tenant, has its own users, groups and roles. In addition to that a designated people can be assigned to manage this directory with very granular permissions depending on what they need to do.

In general, any system that needs to access AAD has to be registered as an AAD application. Applications is another abstraction which allows to set up more granular access to the directory data. A single AAD can have many applications registered, each with it's own permissions, access keys, roles, and permissions.

IFQ registers at least two applications.



Core App

The first "Core AAD App" is intended for backend use. It has been granted enough permissions to both authenticate users and fully manage AAD. Core App can:

- Create/Update/Delete Users

- Create/Update/Delete Groups
- Create/Update/Delete Application Roles
- Authenticate users
- Change user membership in Roles and Groups

IFQ internal services such as API and Orchestration Layer are a part of the Core AAD app so they can perform these operations on request.

External App

External application is created on demand for any application outside of IFQ network, typically this is an API user, including Website or Clinic Portal. They can be two extra applications or the same one.

External application is registered by HFEA in IFQ directory with minimum permission set possible, it can:

- Sign in a user and read profile
- Access Core App (be able to communicate with it)

This gives HFEA flexibility in terms of outsourcing the development of external apps and services as AAD app has its own access keys and not enough permission to do anything dangerous.

Trust

HFEA administrator needs to configure minimum trust so that external application can sign-in users and call core application in Azure Portal on the external application configuration page:

Sign-in

One permission in Microsoft's "Windows Azure Active Directory" application for users to be able to sign-in at all:

The screenshot shows the 'permissions to other applications' section in the Azure Portal. At the top, the 'REPLY URL' is set to 'https://localhost:44300/'. Below this, there are two application entries:

- IFQ Backend**: Application Permissions: 0
- Windows Azure Active Directory**: Application Permissions: 0, Delegated Permissions: 1

A dropdown menu is open for the 'Windows Azure Active Directory' application, showing a list of permissions. The 'Sign in and read user profile' permission is checked, while all other permissions are unchecked.

Access IFQ Core App

One permission to our own Core App which is named "IFQ Backend" in this screenshot:

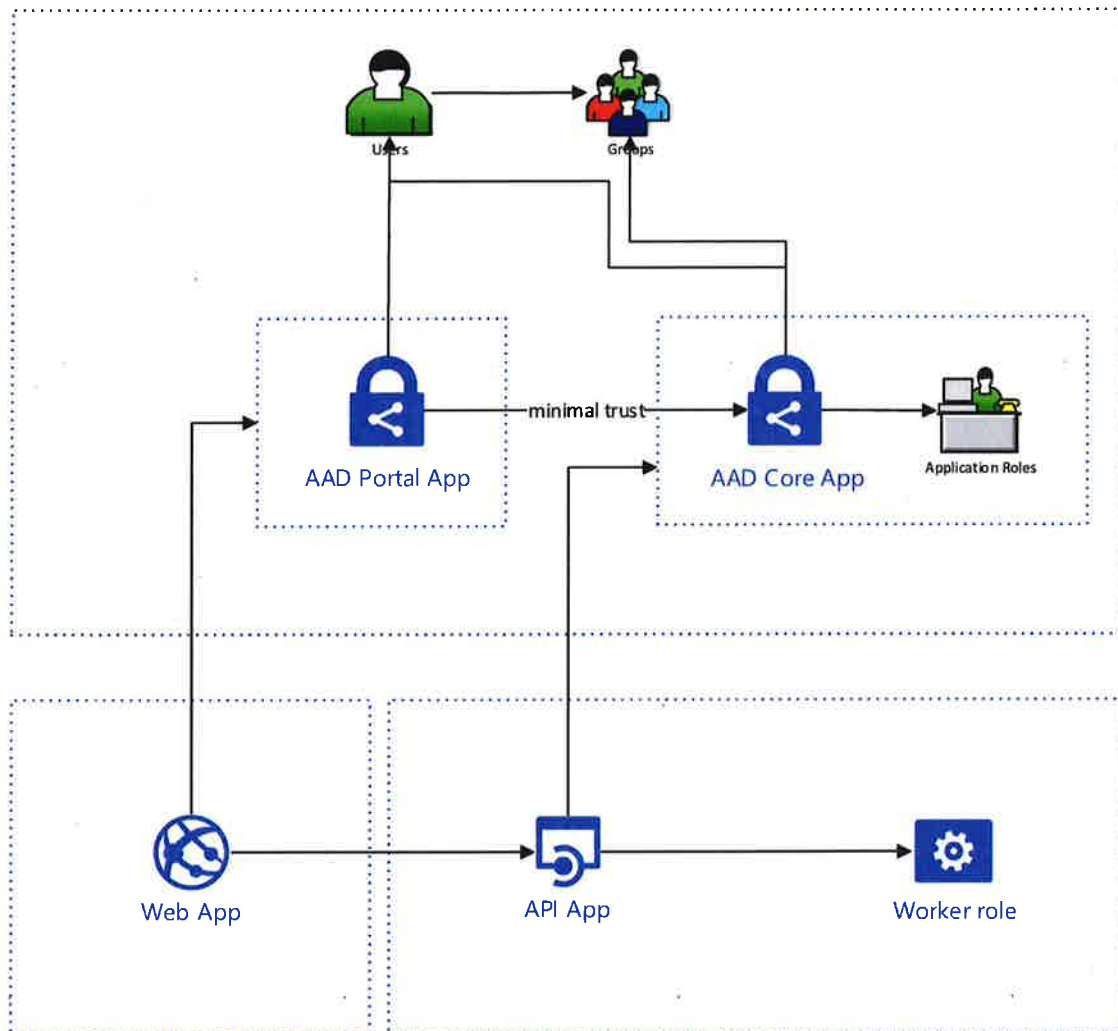
The screenshot shows the 'permissions to other applications' section in the Azure Portal. There are two application entries:

- IFQ Backend**: Application Permissions: 0, Delegated Permissions: 1
- Windows Azure Active Directory**: Application Permissions: 0

A dropdown menu is open for the 'IFQ Backend' application, showing a list of permissions. The 'Access IFQ Grid' permission is checked.

Authentication Sequence

In the diagram below dotted rectangles represent authentication boundaries. In order to cross them a component needs to perform a security operation to have a specific permission.

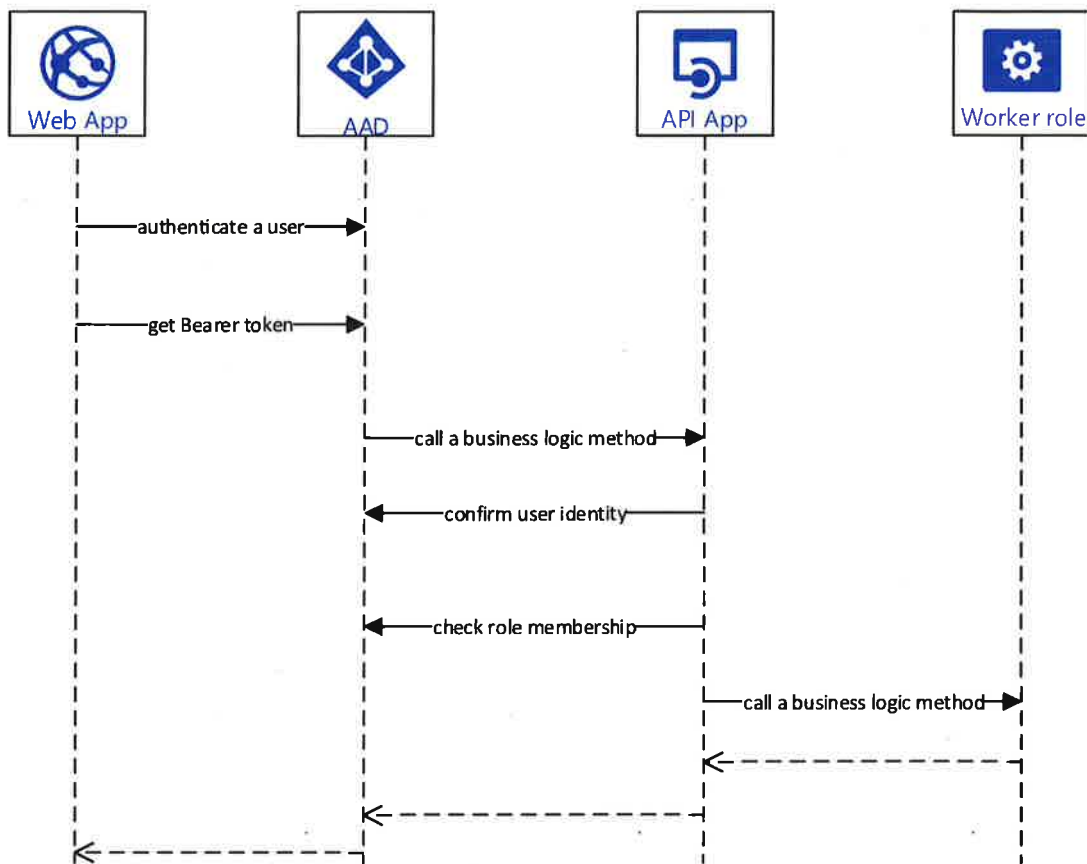


In order for a web site to make a generic call the following authentication parts will be involved:

1. Web App (Website or Clinic Portal) which already has application details for the "AAD Portal App" authenticates a user across IFQ directory. Technically this is done by an OWIN component for ASP.NET MVC supplied by a Microsoft and there is a minimal developer effort.
2. Web App obtains an authentication token and stores session data in browser cookies.
3. Before making the call to API App, Web App calls Azure Active Directory Graph API to obtain a JWT authentication token. Due to the fact HFEA administrator has set up the trust permission AAD returns such a token.
4. Web App uses a simple **Bearer Authentication** to call the Web API. Bearer authentication only requires you to include one extra HTTP header in the call and is supported by most of the web frameworks such as RestSharp.

5. API App validates the JWT bearer token to make sure the user is genuine and authenticates as a user in the Core App.
6. AAD Core App also contains a list of application roles registered for this application. API App performs a check against AAD that the user belongs to an appropriate role and either allows or denies the call. Note that application roles are private to the AAD Core App and external applications don't have access to read them even if they had full permissions in their own app space.

The following diagram illustrates the flow:



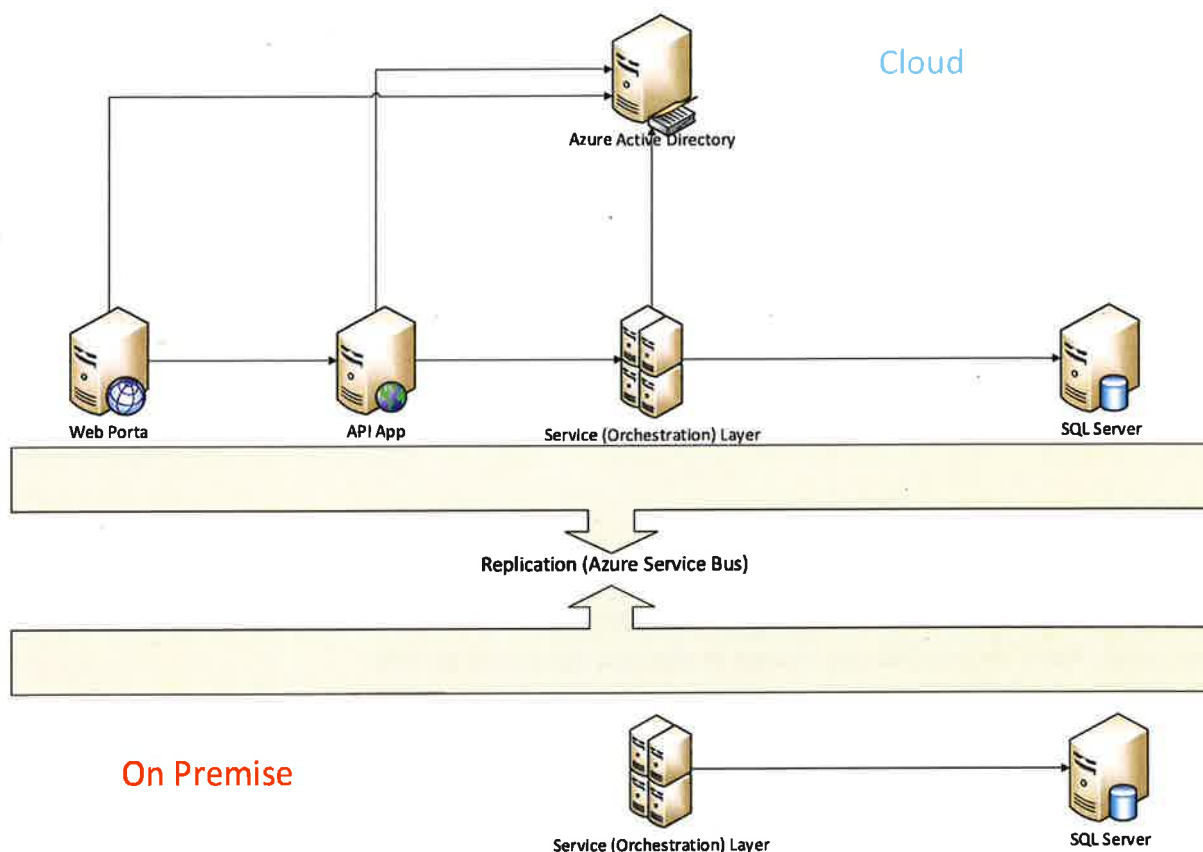
We will provide a full blown easy-to-use authentication library both for internal use and for external developers building applications with ASP.NET MVC.

We will also provide a .NET SDK for calling IFQ REST API, including Bearer authentication support.

Design proposal

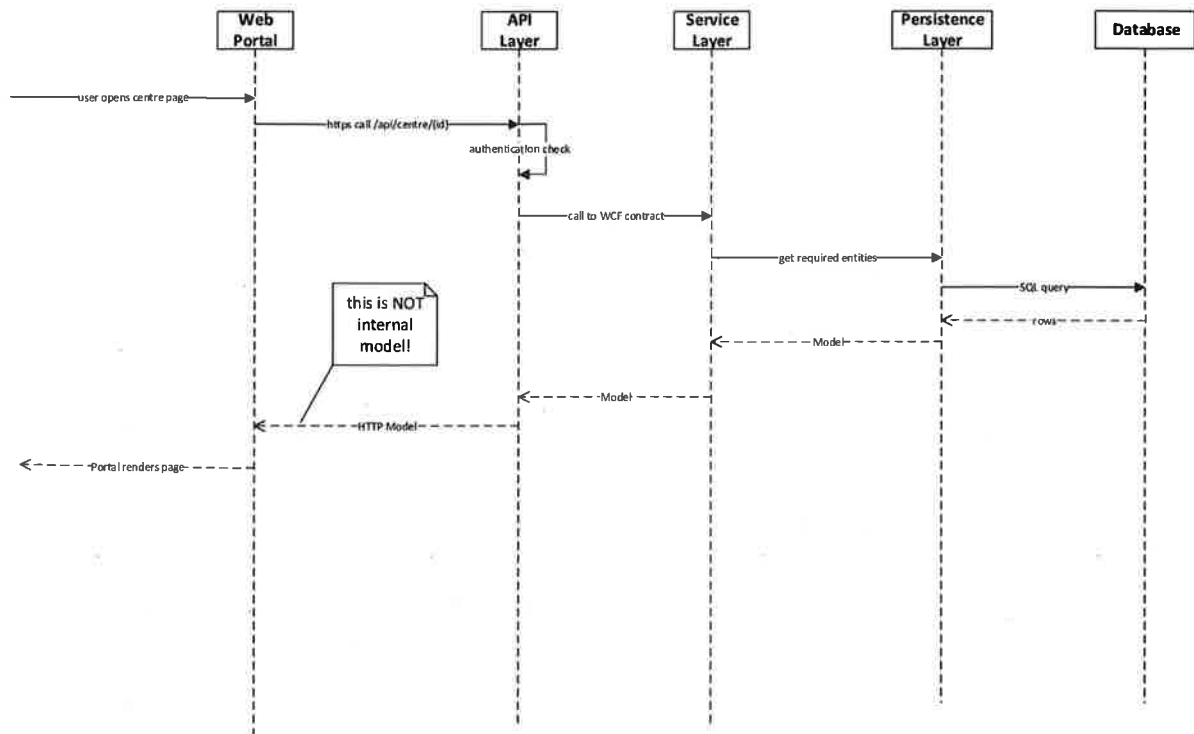
Overview

See the simplified logical structure here:



- **Web Portal.** Developed outside of the scope of this project, is an external caller (such as Umbraco CMS) calling our API App.
- **API App.** The only public-facing service accessible outside of the network. This is an ASP.NET Web API project defining and standardising the public and private API functions available. Potentially this app can be wrapped behind the API Management portal which should be discussed separately.
- **Service (Orchestration) Layer.** Contains all the business logic of the IFQ application. Any API apps or any additional public services must call this layer to perform any business operation. This layer exposes some high-level functionality via its WCF contracts.
- **SQL Server.** Existing sql database with existing tables.

To display a typical web page, the system will involve all the parts in this order:



Due to the fact that parts of the system stays on premise we do replicate some data between the two sides. Azure Service Bus was chosen as the best options to do that.

Solution / Project structure

All the code is written in C#, with the exception of occasional T-SQL stored procedures or queries depending on the application needs. Some code may be written in PowerShell or any other scripting language required for Microsoft Azure deployment scripts.

The solution should have the following projects (approximately):

- **HFEA.Model** – contains all the model classes following the DDD strategy (see below).
- **HFEA.WebApi** – the API app (ASP.NET MVC WebApi with Swagger support). This application uses its own model specific to the REST/SOAP calls it exposes to the public.
- **HFEA.DataLayer** – the data access layer project. Interfaces for accessing the data must be defined in the HFEA.Model project and use the Model in method parameters and return results exclusively. Internally we will use the latest version of the Entity Framework (v6 at the time of this writing). We will utilize code first approach as much as possible here.
- **HFEA.SDK** – contains all the business logic.
- **HFEA.WebPortal** – a test portal which demonstrates some of the functionality of the application, and contains some administration functionality (for example adding users, assigning roles etc.)
- **HFEA.Tests.Unit** – unit tests only.
- **HFEA.Tests.Integration** – integration tests only.

- In addition to this there will be an extra project or two which hosts business logic. Depending on where we host the logic (on premise or in Azure) these can be either Azure Worker Role or a Windows Service application. To test this locally we can use Compute Emulator coming with Azure SDK.

Code Structure

HFEA.Model

Collection of model classes describing IFQ domain and according to DDD:

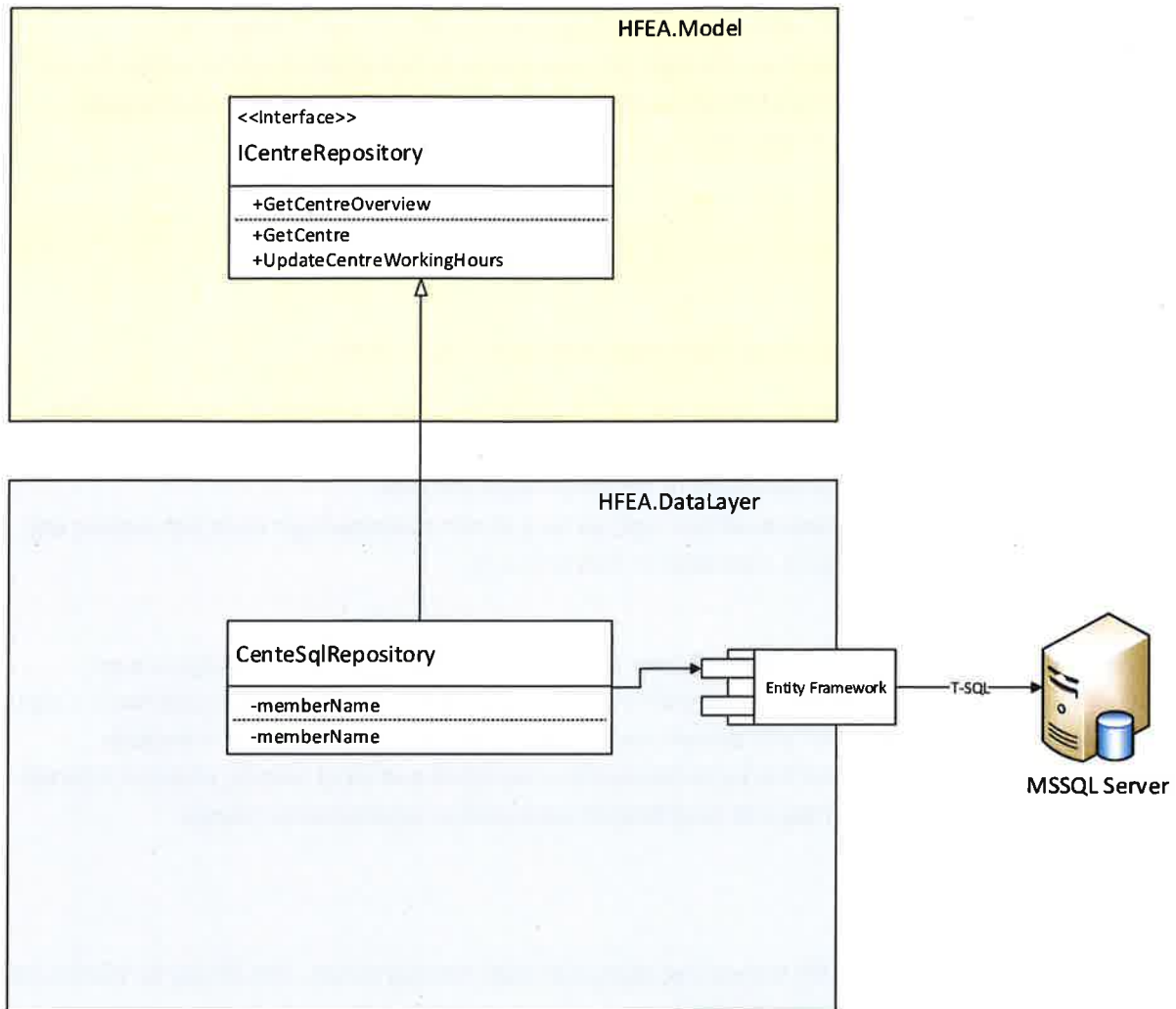
- Not used or exposed in any sense outside of the IFQ solution to external world, including Portal and public website.
- Not compromised by serialisation or database requirements.
- They can and should have business logic, as long as this business logic does not require any external dependencies i.e. database or network calls.

HFEA.WebApi

ASP.NET WebApi application i.e. it *doesn't have a frontend* other than Swagger. Swagger is an industry standard for API discovery, cross platform and widely adopted. This application has it's own model exposed via REST or SOAP and doesn't expose HFEA.Model in any way. This is because external model can't change and has to be backward compatible and dead simple, whereas internal model is rich and is subject to frequent modification as business requirements change.

HFEA.DataLayer

This is a C# library responsible for translating repository calls into sql server. The library is referenced later by a process running the business logic.

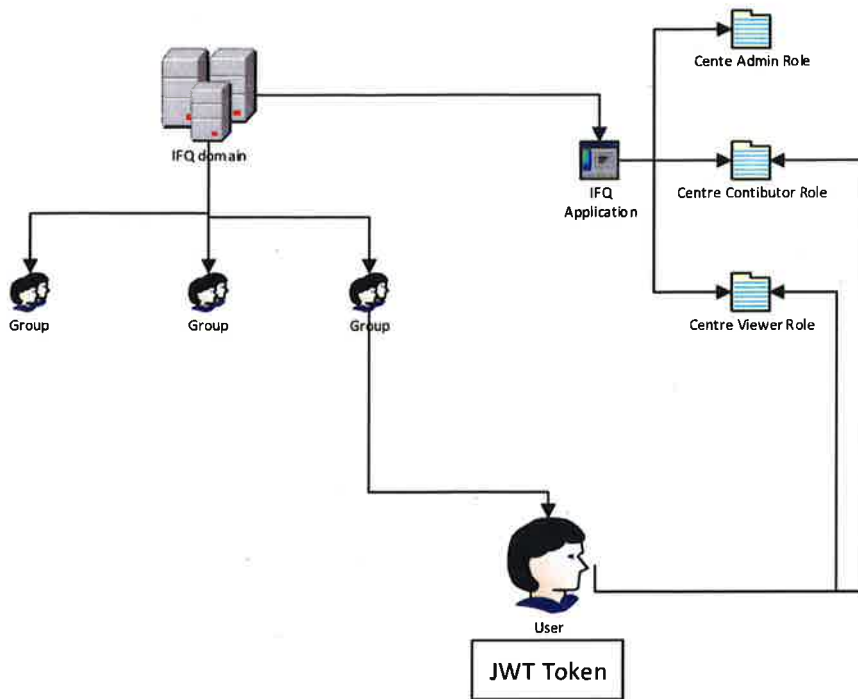


Actual repository interfaces are declared in HFEA.Model and DataLayer only implements them following these practices:

- A repository is a DDD repository with all the attributes implied:
 - Repository does not have any business logic and is only designed to store/retrieve data
 - Repository always operates with Model classes, i.e. repository methods accept model classes as parameters and return model classes as result – it's the DataLayer's responsibility to translate Model into underlying database technology.
- We will use EF6 and code-first to map database to model.

Identity Model

We have chosen Azure Active Directory (AAD) to store user identities. AAD replicates well both with Microsoft Active Directory and third party providers. In addition to that AAD supports modern identity standards such as OpenID Connect and OAuth 2.0, as well as multi factor authentication when required in future.



IFQ Application (see diagram below) is registered in IFQ domain. In terms of AAD application is a separate entity which can hold application specific roles and control user access separate to the primary domain. Application also allow to control directory access in a finer grained way comparing to using the global directory.

IFQ application holds application specific roles which can be added or removed dynamically. Once a user is authenticated against AAD his identity token (JWT – JSON Web Token) carries his identity and roles/groups he belongs to which allows us to do proper authorisation on API calls and other resources.

Authentication scenarios

- Web Portal application developed externally authenticates to AAD itself, then passes the auth token to our API App call which performs authorization checks.
- An external developer authenticates to AAD and passes the token.

Data Replication

It's worth mentioning that data must be replicated only due to the fact that system can't be hosted 100% in Azure Cloud. When this is not the issue we don't need two separate databases on each side and the whole system can use just one single primary replica.

Not all of the data will be replicated, but only a subset required for the API calls. For comparison, there is around 20Gb of SQL table data on premise and only around 300Mb in the cloud.

Database schema (at least for the subset of replicated tables) is identical both on premise and in the cloud, however we don't have to keep SQL server in the cloud and free to choose any technology.

Design decision

- Due to the fact that cloud database may disappear in future as the whole solution potentially can be hosted in Azure Cloud we've decided to keep SQL server and not to use anything more modern. When the physical boundary is removed queries for Azure side should just work with the big on premise database meaning no code changes.

- Due to the fact that the database on premise can be changed by anyone directly avoiding service layer, we don't have a reliable way to intercept the events to send the replication event to the cloud. There are a few options here:
 - Add trigger functions to SQL server which will notify SL on changes so we can push it further.
 - Introduce a call in SL which external callers have to call in order to notify they have changed particular data.
- We still need to see the database in action to make the best architectural decision here.

Logging

All the layers must log as much as possible. Any sort of problem or failure must be able to be replicated in the dev environment by analysing logs.

When there is no preference on any particular logging frameworks I would recommend choosing one of two: log4net or NLog.

Scope for Release 1

- Build a deployable solution which can be pushed to Windows Azure with Continuous Integration.
- Data Replication between cloud and on premise systems. Depending on the complexity and amount of work we may not finish all of it but will build a good framework with best practices.
- Some or all the API calls implemented in all layers. Due to the fact we have no idea how many calls we need to implement or how complex they may be we will do the most.

Methodologies

DDD (Domain Driven Design). DDD is one of the most successful design approaches to tackle easy to most complex problems in building software. The most important principle is that our business domain is described in terms of model classes. DDD is getting even more popular in the Micro services world.

TDD (Test Driven Design). Each new functionality should have a minimal test written before it's implemented. Most suitable frameworks of choice:

- NUnit – general unit/integration test framework
- Moq – mocking framework

HFEA

Release 2 Solution Architecture

Version 1

Ivan Gavryliuk
9-15-2016

Contents

Problem.....	2
Security	3
Authentication	3
Network Security	3
Core Subnet.....	6
SQL Server.....	6
Image Storage	6
Orchestration Layer	8
EPRS Subnet.....	9
Key Authentication	9
Generating HMAC-SHA1 key.....	9
Calling EPRS API with security key	9
Validating EPRS API call on the server	10
IP Address Restrictions.....	10
Internal Subnet	11
EDI Web Application	12
Scaling Options.....	13
Virtual Machines	13
Scaling Up.....	13
Scaling Out	13
EDI Web Application	14

Problem

R2 requires a certain security guarantees which would impact the architecture for the next part of the system. Some of them are:

- Data cannot leave UK premises
- All the systems need to be closed down, except for those which need to be accessed by the public
- All the public system must have a fine grained security rules implemented

Most of the public cloud providers such as Microsoft Azure or AWS do not have physical data centres in the UK which prevents us from hosting data there. However, Microsoft Azure is building one at the moment where we have a private preview access. If that happens the overall architecture and costs are considerably lower than creating a hybrid system.

Generally, HFEA system consists of several basic layers:

- Persistence. Microsoft SQL server (relational data) and large files (binary data).
- Business Logic (Orchestration Layer).
- Public API for EPRS access.
- Clinic Portal Website.
- QA Website.

We use both IaaS and PaaS Azure offerings, balancing between security, support costs, ease of use, and developer productivity.

Also we assume that all of the services are built with .NET Framework and T-SQL.

Security

Authentication

Release 1 (R1) is already using Azure Active directory B2C for authentication (see R1 architecture document for choice decisions). Due to the fact that same users will be able to access R1 and R2 systems it is a natural choice to reuse the same directory. This allows to reuse technology, experience and frameworks built around B2C.

However, QA Website app requires authentication with HFEA Active Directory by internal staff, this is the same directory used to login to Windows or access Office 365 accounts. It is also replicated to Microsoft Azure Active Directory, making it simple to use the Cloud version for authentication from Azure data centre. We assume replication is already configured and is outside of the scope of this document.

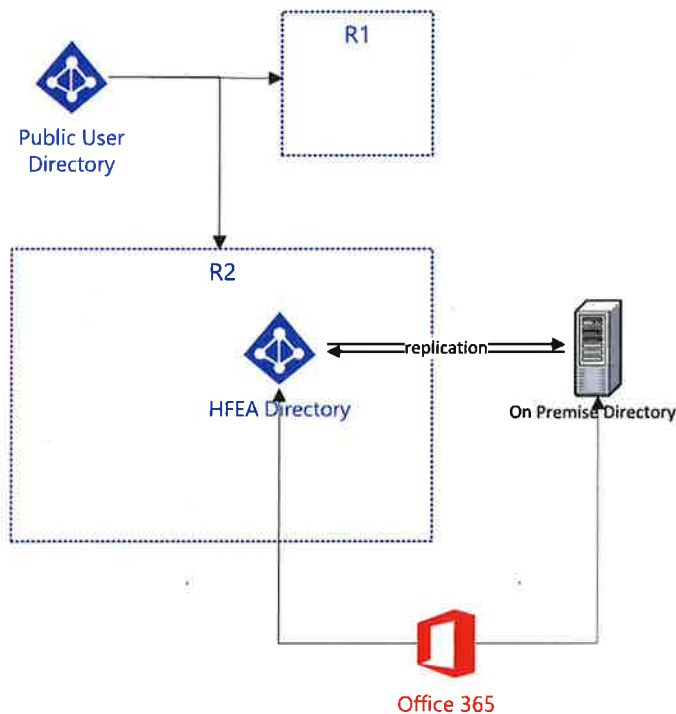


Figure 1 – Active Directory Relationships

Network Security

Considering we are using Azure UK data centre the whole system is hosted physically in the UK. To achieve low latency, high performance and restrict the network from the outside attacks R2 will utilise Azure Virtual Networking technology. It allows customers to replicate physical network in Azure data centres as they would on premise.

Azure Virtual Network is a dedicated workspace for services which is never visible from outside world, unless specifically told by configuring integration with outside world, just like on premise network.

R2 virtual network never talks to HFEA on premise network, and the only piece of information they share is the Active Directory information replicated.

A subnet in a virtual network is a range of IP addresses, with its own security rules and routing tables.

The Virtual Network is divided into 4 subnets (see Figure 2 - Network Diagram):

- **Core.** Contains all the internal (core) services of HFEA application. This subnet does not have outside access from anywhere except for *Orchestration Layer* from other subnets. None of the services in this network have outside internet access. Contained services:
 - Microsoft SQL Server Machine.
 - Orchestration Layer Service.
 - Image Storage.
- **EPRS.** Hosts Public REST API used by EPRS providers.
- **Internal.** Contains QA Web Application used exclusively by internal HFEA staff. Theoretically it could live in the Core subnet, however for easier access management it is recommended to create a separate subnet.
- **Gateway Subnet.** This subnet is used only for administrative access to the parts of the system and can be accessed by individuals using Azure VPN Gateway. Required mostly for troubleshooting and access by software developers. Note that this subnet doesn't have NSG attached which is a requirement for VPN connection to work properly in Azure.

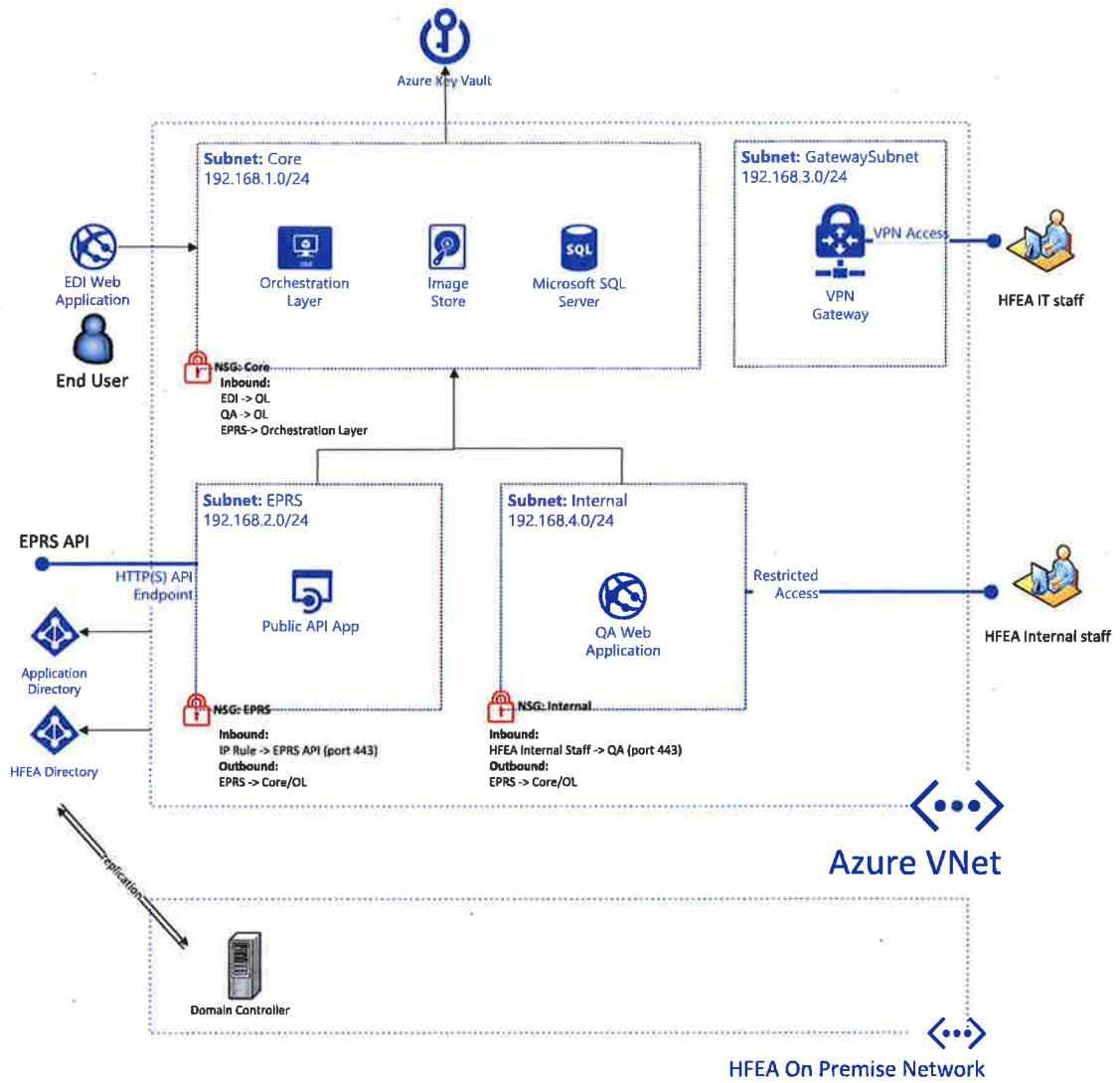


Figure 2 - Network Diagram

Core Subnet

Due to the geographical limitations that data must not leave the UK and be encrypted at rest we cannot use traditional Azure Storage or Azure SQL Server.

SQL Server

We will rent a Virtual Machine with SQL Server 2014 SP1 from Azure Marketplace on PAYG license which is a usual VM with all capabilities a normal VM has. This can be joined to our Virtual Network in Storage subnet with restricted access only by Orchestration Service from the Business Logic subnet. SQL Server database is encrypted¹ using Transparent Data Encryption² (TDE) for IaaS instances. Encryption has to be configured manually after installing SQL Server instance³.

Image Storage

Image Storage is a set of files falling under the same security restrictions. There are two major options in Azure to protect file data:

1. **Azure Storage Service Encryption for Data at Rest** enables encryption on blob storage on the Azure Cloud side. Encryption is handled
2. **Azure Disk Encryption**. Encrypts OS and data disks on a VM level using BitLocker on Windows or DM-Crypt on Linux. Raw data never leaves VM boundaries and customer secrets are stored in Azure Key Vault service. It is the safest choice for maximum security.
3. **Custom Encryption**. Involves writing a software component in the Orchestration Layer for handling encryption from the software.

Table below outlines the pros and cons of every approach.

	Azure Storage	Azure Disk Encryption	Custom Encryption
Encryption at Rest	Yes	Yes	Implementation
Transport Encryption	HTTPS only	Not applicable	Implementation
Implementation Effort	Trivial	Hard (infrastructure configuration)	Hard (developer resources)
Deployment Effort	Trivial	Hard	Trivial
Encryption Method	AES 256	AES 256 (BitLocker)	Implementation
Overall Security	Medium	High	Medium-High
Scalability	Up and Out	Up Only	Up and Out

Based on the comparison and requirements I would strongly recommend implementing storage with Azure Disk Encryption. Read more: <https://azure.microsoft.com/en-gb/documentation/articles/azure-security-disk-encryption/>.

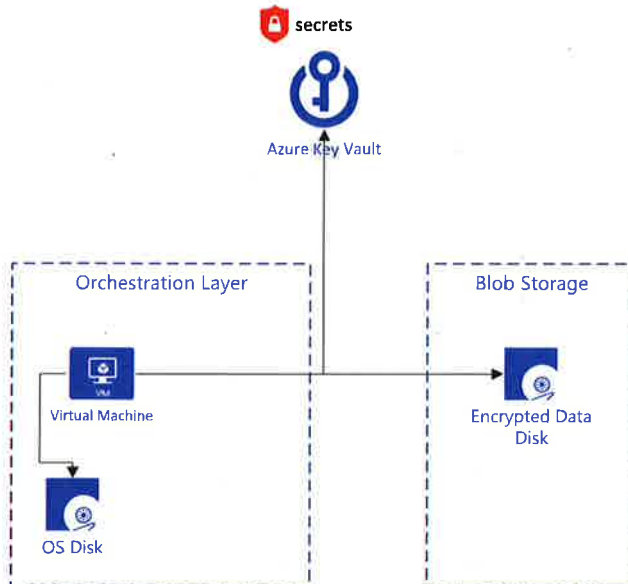
This is not a scripted process and has to be configured manually.

¹ SQL Server Encryption, <https://msdn.microsoft.com/en-us/library/bb510663.aspx>

² Transparent Data Encryption, <https://msdn.microsoft.com/en-us/library/bb934049.aspx>

³ Configuring SQL Server Encryption, <https://blogs.technet.microsoft.com/kv/2015/01/12/using-the-key-vault-for-sql-server-encryption/>

In essence when configuring a disk encryption a new data disk is attached to Orchestration Layer machine with a new drive letter. Software running on this machine can access the drive as it would normally do and configured Windows OS takes care encrypting and decrypting data on the go.



One of the limitations of this approach is it's not scalable for the reason that a disk cannot be shared between two or more instances of virtual machines. For that reason, Orchestration Layer machine can only be scaled up.

When workload will reach a certain limit in future OL can be moved to a separate VM instance and existing instance can act as a file server freeing up resources for the actual business logic processes.

In order to scale even more you can implement custom encryption in the Orchestration Layer endpoint which will allow to scale out infinitely, but none of the scaling options are included in this release implementation.

Orchestration Layer

Unlike R1 where Business Logic was hosted in an Azure Cloud Service we can't do this anymore, because Cloud Services have a public access and require creating a public IP address for communication purposes. There are many options available to solve this problem, however considering a low load and security restrictions the most appropriate one is using Azure Virtual Machines. There are a few pros and cons to using VMs.

Pros:

- Cloud provider agnostic, every single cloud provider supports Virtual Machines and running executables which is what a windows service is.
- Flexibility when configuring security and installing custom software.
- Lower cost comparing to other alternatives.

Cons:

- Management overhead comparing to Cloud Services or Service Fabric.
- No auto deployment built-in (but you can utilise existing *Octopus Deploy*⁴ instance)

In the first release we will use one virtual machine, however you must consider scaling options (see the section) before going to production or when performance is going bad.

Orchestration Layer is a Microsoft Windows Service application running in a background and hosting all the business logic and model. Other layers provide only integration or user interface services.

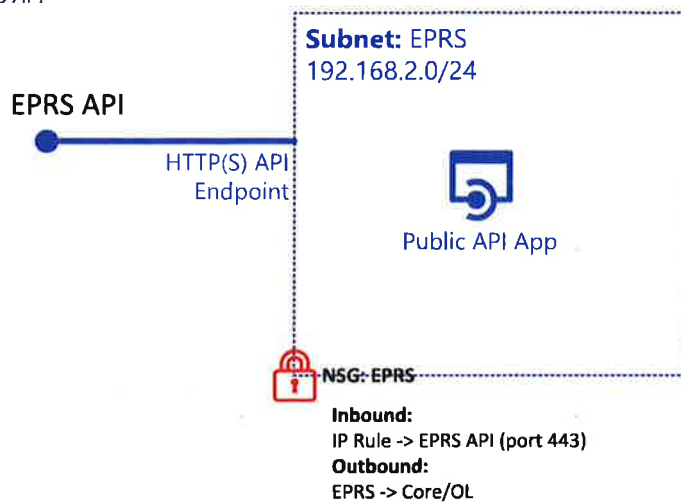
Orchestration Layer both hosts services for API or internal applications via Windows Communication Foundation (WCF) and performs long-running background tasks when needed.

There are no special security requirements for OL VM, it doesn't have outbound Internet access and only needs to access SQL server database.

⁴ Octopus Deploy, <https://octopus.com/>

EPRS Subnet

Figure 3 - EPRS API



EPRS API lives in a separate subnet only for security reasons. EPRS provide API access for external clients to their dedicated centres and have a key-based authentication. In addition to that EPRS service has only port 443 (HTTPS) open for internal calls.

HFEA is responsible for giving out keys to the EPRS customers. Every key has access to only one single centre. For increased simplicity and cross platform support (we suppose that EPRS clients can use a multitude of different client platforms) we recommend using Hash-Based Message Authentication Code (HMAC) with SHA-1 algorithm which is still considered to be secure and performing well.

Key Authentication

Generating HMAC-SHA1 key

In Windows Server the key can be generated by calling to Cryptography API, see [MSDN Documentation](#). The key then must be assigned to the client by putting in SQL Server database on HFEA side and transferring to EPRS user.

Calling EPRS API with security key

In order to call EPRS client have to sign their request before issuing. The signature is generated in a few steps:

1. Get the current clock time in UTC – T.
2. Get your centre ID – C.
3. Format a signature string as "C:T".
4. Compute HMACSHA1 hash of the signature string using your key and represent as a BASE64 encoded string.
5. Add HTTP header "x-hfea-date" to request. Note that you have to agree on time format on both client and server side, the most common is (C# example):
T.ToUniversalTime().ToString("ddd, dd MMM yyyy HH:mm:ss UTC");

6. Add HTTP header "x-hfea-signature" to request by setting the value of the string computed in step 4.

Validating EPRS API call on the server

The validation can be performed in a few simple steps too:

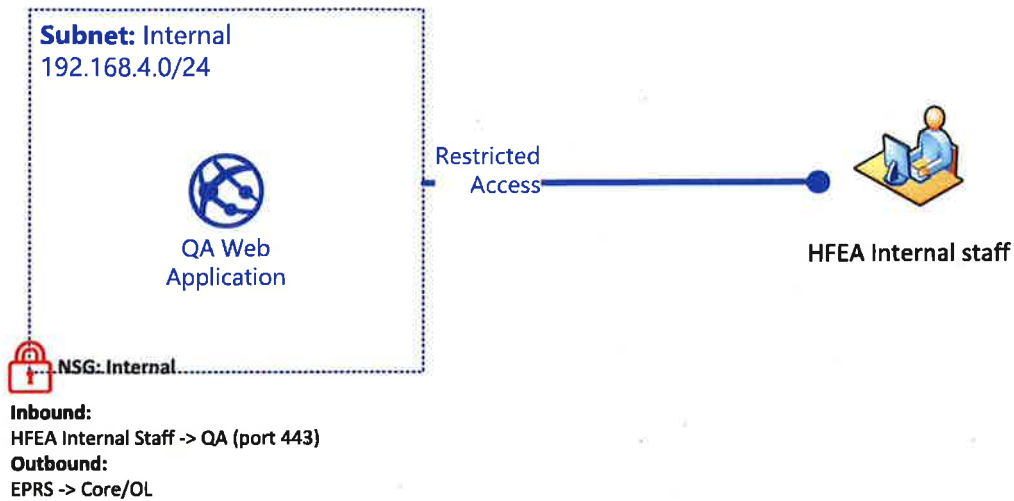
1. Check that both "x-hfea-date" and "x-hfea-signature" is present, otherwise reply with 401 (Unauthorized) code.
2. Take the current clock time and compare to "x-hfea-date" to check if they differ a lot. If the difference is more than 1-minute reply with 401.
3. Compute HMACSHA1 hash of the request following steps 1, 2, 3, 4 in "Calling EPRS API with secure key" section. Remember to take "x-hfea-date" for date value as current clock will be different from client's clock.
4. Validate if your hash is matching client's hash. Deny authentication if they aren't and allow otherwise.

IP Address Restrictions

In order to restrict access from certain IP addresses or ranges a built-in functionality of Network Security Group EPRS can be used to create Inbound Access Rules⁵.

⁵ Managing Network Security Groups in Azure, <https://azure.microsoft.com/en-gb/documentation/articles/virtual-networks-create-nsg-arm-portal/>

Internal Subnet



This subnet hosts internal QA Application accessed exclusively by HFEA Staff.

For authentication it uses Azure Active Directory replicated from the on-premises directory. It is not to be confused with Application Directory used to access the system from the Internet.



QA Web Application is also an IIS hosted solution on Windows Azure VM.

It has a direct access to Orchestration Layer from the *Core* subnet to interact with data. The access is controlled by Network Security Groups.

EDI Web Application



Is another part of IFQ visible from outside (the other one is EPRS API). It's hosted as a PaaS solution on Azure Platform⁶. PaaS is possible in this case because the target audience is internet facing and there are no special security requirement except for a strong authentication.



End User

Due to the fact we are using Azure B2C to offshore authentication process it's satisfied too.

Having this hosted as PaaS also gives us better flexibility in terms of scaling, deployment and monitoring.

EDI connects directly to the Orchestration Layer by connecting to our Virtual Network⁷.

⁶ Azure Web Apps, <https://azure.microsoft.com/en-gb/documentation/articles/app-service-web-overview/>

⁷ Integrate your app with Azure Virtual Network, <https://azure.microsoft.com/en-gb/documentation/articles/web-sites-integrate-with-vnet/>

Scaling Options

Virtual Machines

Most of the services are hosted inside virtual machines, which have two major scaling approaches.

Scaling Up

Scaling up involves adding more virtual resources depending on where the bottleneck is in current performance scenario (CPU, Disk, Memory etc.). You can rescale the machine instance in Azure Portal.

Scaling Out

Scaling up is not a perfect option and always comes with it's drawbacks:

- During scaling up virtual machine goes offline for a short period of time, and needs warming up again to start your hosted application
- Scaled up instances are expensive, as they always billed for provisioned resources regardless whether they are in use
- Scaled up instances can't provide enough continuity – when the service fails a manual intervention is required.

Scaling out comes to the rescue and covers all the bad points. Essentially scaling out means cloning a virtual machine to run two or more instances. Every instance has its own virtual internal IP address, regardless whether it's public or private facing.

Client of scaled out instances are not aware of the change; they are calling a virtual endpoint called a Load Balancer. Load Balancers can be internal or external, which only indicates which sort of IP address they are assigned to (public or private). For instance, Orchestration Layer will use internal load balancer as it's not publicly visible from the Internet, whereas all of the remaining services are using External Load Balancer.

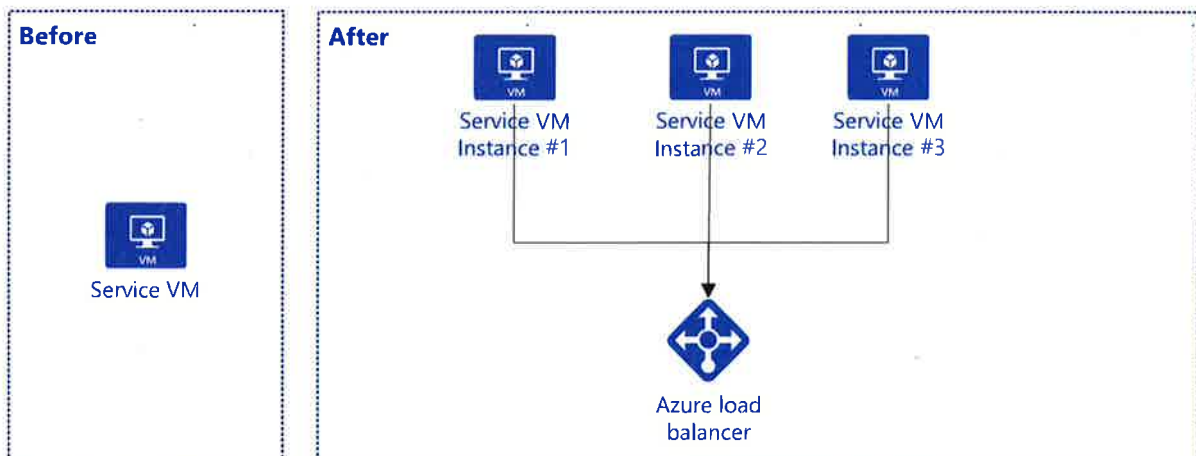


Figure 4 - Without and With Scaling out

EDI Web Application

This application is hosted inside Azure App Service container, therefore scaling is trivial as it's baked into App Service package and works out of the box⁸.

⁸ Scaling Out Application Plans, <https://azure.microsoft.com/en-us/documentation/articles/insights-how-to-scale/>

Public Interest Disclosure ("Whistleblowing") Policy

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

Details:

Meeting	AGC
Agenda item	14
Paper number	AGC (07/12/2016) 520 HR
Meeting date	7 December 2016
Author	Rachel Hopkins, Head of Human Resources

Output:

For information or decision?	For decision
Recommendation	The Committee is asked to agree the amended policy.
Resource implications	None
Implementation date	Ongoing
Communication(s)	Ongoing
Organisational risk	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High

Annexes

Annex A –	Whistleblowing Policy
-----------	-----------------------

1. Purpose

- 1.1.** The Public Interest Disclosure Policy generally referred to as the “Whistleblowing” Policy was implemented to ensure people working for the HFEA were aware of the channels available to report inappropriate behaviour.
- 1.2.** This paper also confirms that a review of the HFEA Whistleblowing Policy has been undertaken and to set out the updated policy which includes a few minor amendments for the committee's agreement..

2. Policy

- 2.1.** The policy was shared with the Staff Forum and tabled at CMG who approved the draft policy. In December 2014, the Committee approved it. A number of minor amendments that have been proposed.
- 2.2.** A review was not undertaken in 2015 due to staff and work commitments and therefore was not presented to AGC for approval.
- 2.3.** We have now reviewed the policy and have updated names where appropriate and re-branding.
- 2.4.** Any comments or changes the Committee deems necessary are requested.

Public Interest Disclosure ("Whistleblowing") Policy

1. Introduction

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

2. Aim

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

3. Scope

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

4. Responsibility

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

5. Principles

- 5.1 Employees who raise their concerns within the HFEA, or in certain circumstances, to prescribed external individuals or bodies will not suffer detriment as a result of their disclosure, this includes protection from subsequent unfair dismissal, victimisation or any other discriminatory action.
- 5.2 The Public Interest Disclosure Act 1998, (more widely known as the 'Whistleblowers' Act) protects 'workers' from suffering any detriment where they make a disclosure of information while holding a reasonable belief that the disclosure tends to show that:
- (a) a criminal offence has been committed, is being committed or is likely to be committed,
 - (b) a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject,
 - (c) A miscarriage of justice has occurred, is occurring or is likely to occur,
 - (d) The health and safety of any individual has been, is being or is likely to be endangered,
 - (e) The environment has been, is being or is likely to be damaged, or
 - (f) Information tending to show any matter falling within any one of the preceding paragraphs has been, is being or is likely to be deliberately concealed.
- 5.4 It should be noted that disclosures, which in themselves constitute an offence, are not protected.

- 5.4 HFEA's policy is intended to ensure that where a member of staff, including temporary or contractual staff, have concerns about criminal activity and/or serious malpractice e.g. fraud, theft, or breaches of policy on Health and Safety, they can be properly raised and resolved in the workplace. Such matters **must be raised internally** in the first instance. Please refer to the paragraph on gross misconduct in the Authority's Disciplinary Policy, and also the Authority's Fraud and Anti-Theft Policy.
- 5.5 HFEA seeks to foster a culture that enables staff who witness such malpractice to feel confident to raise the matter in the first instance in the knowledge that, once raised, it will be dealt with effectively and efficiently. The HFEA will not tolerate the victimisation of individuals who seek to bring attention to matters of potentially serious public concern, and will seek to reassure any individual raising a concern that he or she will not suffer any detriment for doing so. If an individual is subject to a detriment for raising a concern the HFEA will seek to pursue an appropriate sanction.
- 5.6 Frivolous or vexatious claims which fall outside the protection of the Act or such other provisions as may be held to protect them (e.g. HFEA's codes of conduct, confidentiality clause etc.) may be considered acts of misconduct and subject to disciplinary action.
-

6. Procedure

Internal Disclosure

- 6.1 HFEA staff who become concerned about the legitimacy or public interest aspect of any HFEA activity or management of it should raise the matter initially with their line manager. If a member of staff feels unable to raise the matter through their line manager, they may do so through the HR Department.
- 6.2 It will be the responsibility of the line manager to record and pursue the concerns expressed; consulting such other parts of the Authority; (e.g. HR, SMT) as may be necessary, including where appropriate consideration as to whether external expert assistance is required.
- 6.3 The identity of the individual making the disclosure will be kept confidential if the staff member so requests unless disclosure is required by law.
- 6.4 In other than serious cases, the line manager will normally be responsible for responding to the individual's concern. They must maintain appropriate records and ensure that they provide the individual raising the concern with:
- An explanation of how and by whom the concern will be handled
 - An estimate of how long the investigation will take
 - Where appropriate, the outcome of the investigation
 - Details of who he/she should report to if the individual believes that he/she is suffering a detriment for having raised the concern
 - Confirmation that the individual is entitled to independent advice.

- 6.5** Should a member of staff feel that they are not satisfied that their concern has been adequately resolved, they may raise the matter more formally with the Chief Executive.
- 6.6** Any member of staff wishing to make a disclosure of significant importance may approach the Chief Executive in the first instance. Matters of significant importance include, but are not restricted to, criminal activity e.g. fraud or theft, or other breaches of the law; miscarriage of justice; danger to health and safety; damage to the environment; behaviour or conduct likely to undermine the Authority's functions or reputation; breaches of the *Seven Principles of Public Life* (Annex A) and attempts to cover up such malpractice.
- 6.7** The matter of significant importance may have taken place in the past, the present, or be likely to take place in the future.
- 6.8** Concerns may be raised either in writing or at a meeting convened for the purpose. A written record of meetings must be made and agreed by those present. In serious cases or in any case where a formal investigation may be required, line managers concerned should consult the Head of HR and SMT, unless they are implicated, when they should speak to the Chair. Line managers must not take any action which might prejudice any formal investigation or which might alert any individual to the need to conceal or destroy any material evidence.
- 6.9** Where an individual has reason to believe that the concerns about which he / she intends to make a disclosure are condoned or are being concealed by the line manager to whom they would ordinarily be reported, the matter may be referred directly to the Head of HR who will determine in conjunction with the Chief Executive the need for, and the means of, investigation. In exceptional circumstances, the Head of HR may take the disclosure directly to the HFEA Chair. Any such approach should be made in writing, clearly stating the nature of the allegations.
- 6.10** Unless inappropriate in all the circumstances, investigations will normally be undertaken by the following posts:

<i>Allegation against</i>	<i>Investigated by</i>
Directors	Chief Executive
Chief Executive	Chair
Member	Chair
Audit Committee Member	Audit Committee Chair
Chair	Department of Health*
Deputy Chair	Chair

*Via Senior Sponsor at the DH (currently Mark Davies, Director, Health Science and Bioethics (tel. 0207 210 6304^[MA1] / mark.davies@dh.gsi.gov.uk)

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

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

External Disclosure

- 6.13 The HFEA recognises that there are circumstances where the matters raised cannot be dealt with internally and in which an individual may make the disclosure externally and retain the employment protection of the Act. Ordinarily such disclosure will have to be to a person or regulatory body prescribed by an order made to the Secretary of State for these purposes.
- 6.14 Prescribed bodies under the Act include the Comptroller and Auditor General of the National Audit Office (NAO), who are the external auditors to the Authority. The Act states that disclosure to the NAO should relate to “the proper conduct of public business, fraud, value for money and corruption in relation to the provision of centrally-funded public services.”
- 6.15 The NAO have a designated whistle blowing hotline which can be used in confidence on 020 7798 7999. Further information about this service and other bodies prescribed under the Act is available via the NAO’s website: <http://www.nao.org.uk/contact-us/whistleblowing-disclosures/>
- 6.16 In these circumstances the worker will be obliged to show that the disclosure is made in good faith and not for personal gain, that he or she believed that the information provided and allegation made were substantially true, and that they reasonably believed that the matter fell within the description of matters for which the person or regulatory body was prescribed.
- 6.17 Unless the relevant failure of the employer is of an exceptionally serious nature, the worker **will not** be entitled to raise it publicly unless he/she has already raised it internally, and/or with a prescribed regulatory body and, in all the circumstances, it is reasonable for him / her to make the disclosure in public.
- 6.18 If a member of staff is unsure of their rights or obligations and wishes to seek alternative independent advice, Public Concern at Work is an independent organisation that provides confidential advice, free of charge, to people concerned about wrongdoing at work but who are not sure whether or how to raise the concern (telephone 020 7404 6609 or 020 3117 2520, email: whistle@pcaw.org.uk), or visit their website at <http://www.pcaw.org.uk/>. HFEA staff may also use the Whistleblowing Helpline, which offers free, confidential and anonymous advice to the health sector: <http://wbhelpline.org.uk/>
- 6.19 Where matters raised from external disclosure procedures are (as appropriate) subsequently investigated and resolved internally, a written record of the matters raised and actions taken should be forwarded to the Chair for inclusion in the central record of issues referred under this policy. The anonymity of the individual who made the disclosure should be preserved as far as possible.

Information held on the HFEA Register

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

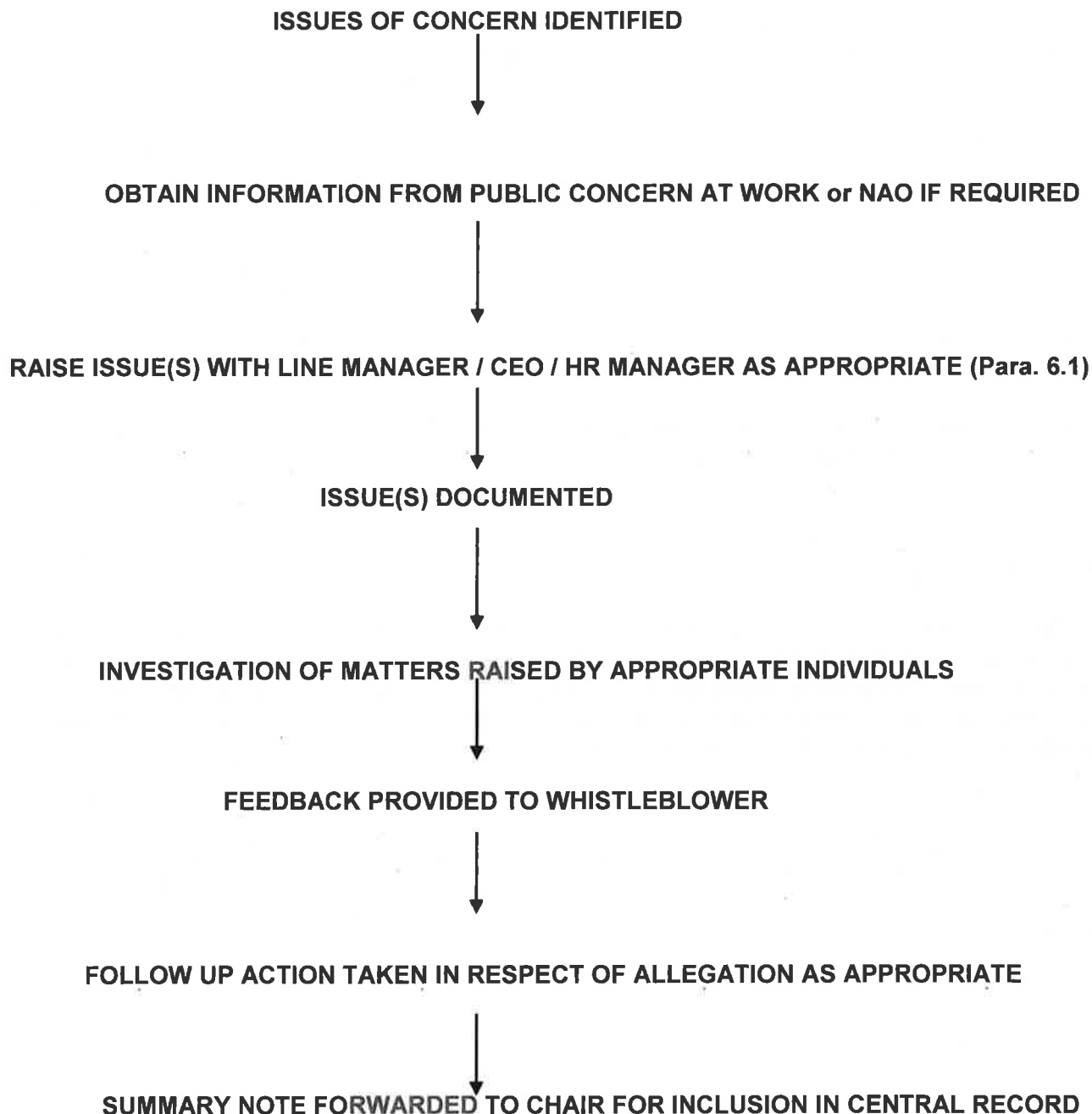
7. Notes

- 7.1 This policy will be reviewed by the Audit and Governance Committee annually.
- 7.2 An anonymised summary of issues raised under this whistleblowing policy and remedial actions taken will be forwarded annually to the Authority for information.
- 7.3 The role of the HFEA as a regulatory body:

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

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

Procedure Diagram



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

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

Seven Principles of Public Life (The as recommended by the Nolan Committee)

Selflessness

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

Integrity

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

Objectivity

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

Accountability

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

Openness

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

Honesty

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

Leadership

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

These principles apply to all aspects of public life.

Document name	Public Interests Disclosure
Doc Ref No.	2014/021228
Release date	10 December 2014
Author	Head of HR
Approved by	CMG/AGC/Staff Forum
Next review date	December 2015
Total pages	9

Version/revision control

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

Annual review of committee effectiveness

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

Details:

Meeting	Audit and Governance Committee
Agenda item	16
Paper number	[AGC (07/12/2016) 521 SK]
Meeting date	7 December 2016
Author	Siobhain Kelly

Output:

For information or decision?	Information and comment.
Recommendation	AGC is invited to consider and comment on the Committee's effectiveness, using the supplied NAO checklist as a basis for discussions
Resource implications	In budget.
Implementation date	Any suggested changes to be fed into annual review of standing orders, reported to Authority in March 2017
Organisational risk	<input checked="" type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High
Annexes	Annex 1: NAO checklist for Audit Committees

1. Introduction

- 1.1. It is now an established process for the HFEA's committees to conduct a review of their effectiveness annually. Such reviews are conducted in the autumn, with the results feeding in to the Authority, along with any changes to Standing Orders, in the following spring. While other HFEA committees have standard internal proformas as a guide to their annual review, the Audit and Governance Committee uses the NAO's Audit Committee checklist (at annex A) as a guide for its review.
- 1.2. This NAO checklist has not been updated since the committee used it for its annual review in 2015.
- 1.3. This paper provides some prompts on the matters committee members may wish to reflect upon regarding the activities and performance of the committee in the past year.

2. Committee meetings, functions and agendas

- 2.1. Since the last annual review in 2015, the Committee has met four times, as planned. The Committee has been quorate at all meetings, and had a full complement of four members at two meetings. In addition, observers or representatives from DH have been present. Both internal and external auditors were represented at all meetings. The committee had recognised the challenge of achieving quoracy and has recently increased its membership to five, to reduce the burden on the existing members.
- 2.2. After a year of change (2014, with a new Chair and Director of Finance and Resources) this year has been one of stability and building capacity. Apart from the usual items taken to AGC, focus has been put on providing assurance for the IfQ project. Further work has been undertaken on a move to risk assurance mapping, which will continue in the future. Delegated powers and functions appear to be appropriate and lines of communication with the Authority will have improved with a formal report each year. There are two ongoing actions from last year's review – external member attendance at inspections and Authority meetings – which are dependent on members' availability.

3. Recommendation

- 3.1. The NAO checklist is seen as a guide for all public sector organisations, from the largest to the smallest, and therefore and must be applied in a proportionate way. It is not intended as having to be fully completed by every committee regardless of the organisations size; rather, it acts as a prompt for committees to follow in conducting their reviews.
- 3.2. AGC is invited to consider the NAO checklist in advance of the 7 December meeting, and feed back views at that meeting. The Head of Corporate Governance (interim) will capture views during the meeting, before circulating a final report for agreement remotely after the meeting.

GOOD PRACTICE

The Audit Committee self-assessment checklist

2nd edition January 2012

Financial Management and Reporting

Our vision is to help the nation spend wisely.

We apply the unique perspective of public audit to help Parliament and government drive lasting improvement in public services.

The National Audit Office scrutinises public spending for Parliament and is independent of government. The Comptroller and Auditor General (C&AG), Amyas Morse, is an Officer of the House of Commons and leads the NAO, which employs some 860 staff. The C&AG certifies the accounts of all government departments and many other public sector bodies. He has statutory authority to examine and report to Parliament on whether departments and the bodies they fund have used their resources efficiently, effectively, and with economy. Our studies evaluate the value for money of public spending, nationally and locally. Our recommendations and reports on good practice help government improve public services, and our work led to audited savings of more than £1 billion in 2011.

Contents

Introduction 4

Section I

Good practice principles for Audit
Committees **6**

Section II

The role of the Chair: good practice **21**

Section III

Committee support: good practice **24**

Introduction

1 This Checklist¹ has been designed to help Audit Committees in central government assess how well they apply good practice. The criteria we have used are derived largely from the Audit Committee Handbook (March 2007)² published by HM Treasury.

2 The Handbook highlights five good practice principles which aim to answer the following key questions:

- **Principle 1: The Role of the Audit Committee** – Does the Audit Committee effectively support the Board and the Accounting Officer by reviewing the completeness of assurances to satisfy their needs, and by reviewing the reliability and integrity of these assurances?
- **Principle 2: Membership, Independence, Objectivity and Understanding** – Is the Audit Committee suitably independent and objective, and does each member have a good understanding of the objectives, priorities and risks of the organisation, and of their role on the Audit Committee?
- **Principle 3: Skills** – Does the Audit Committee contain or have at its disposal an appropriate mix of skills to perform its functions well?
- **Principle 4: Scope of Work** – Is the scope of the Audit Committee suitably defined, and does it encompass all the assurance needs of the Board and Accounting Officer?
- **Principle 5: Communication** – Does the Committee engage effectively with Financial and Performance Reporting issues, and with the work of internal and external audit? And does the Audit Committee communicate effectively with the Accounting Officer, the Board, and other stakeholders?

3 For each principle, we have developed a series of Good Practice Questions to help Audit Committees conclude whether they are meeting these principles. These are set out in **Section I** of this checklist.

4 In addition, the role of the Chair and the provision of appropriate secretariat support are key for an effective Audit Committee. The Handbook details Good Practice Questions on these two roles. **Sections II** and **III** of this checklist include questions that will enable the Audit Committee to determine if they currently meet this guidance.

¹ This Checklist was originally published in November 2009 and has been updated (January 2012) to reflect the requirement for departments, their executive agencies and arm's-length bodies to produce a Governance Statement in place of the Statement on Internal Control in their annual report and accounts for 2011-12 onwards. Guidance on the Governance Statement is set out in the revised Chapter 3 of Managing Public Money (HM Treasury, 2011)

² *Corporate governance in central government departments: Code of good practice* (HM Treasury, July 2011) provides that Audit Committees should be established and function in accordance with the *Audit Committee Handbook* (HM Treasury, March 2007).

How to use this Checklist

5 To help Audit Committees conclude as to whether they are meeting the Principles highlighted above, we have developed Good Practice Questions to inform the thinking process. These Questions are phrased to identify 'yes', 'no' or 'not applicable' responses.

6 We recognise, though, that organisations and their Audit Committees vary considerably in their size and in the complexity of issues that they deal with. In some circumstances, it may therefore be more appropriate to only use the more important Questions to help inform debate – and we have highlighted these in **bold**.

7 Also, the checklist is not exhaustive, and should the Audit Committee or their organisation feel that they have experience of other good working practice that will make the Committee work more effectively, they should not be deterred from implementing these practices, after consulting with the Board, if appropriate.

NAO Facilitated Workshops

8 To help Audit Committees use this checklist, the National Audit Office, as part of its performance improvement work, offers **Facilitated Workshops** for Audit Committees to help them use a tailored version of this checklist and draw conclusions as to their effectiveness. In this way, the workshop provides an opportunity for individual Audit Committees to work together, away from their normal business, to assess how well they work and establish areas to develop further. The workshop is followed up with an Action Plan that draws from the decisions and actions raised. This Action Plan will be owned by the Audit Committee, and act as the means by which decisions are implemented and reviewed.

9 If you would like the NAO to facilitate a workshop for your Audit Committee, please ask your usual NAO contact or Client Lead.

10 This checklist is also available as a Word document to enable Audit Committees to record their responses electronically.

National Audit Office

November 2009

Section I

Good practice principles for Audit Committees

Principle 1: The role of the Audit Committee

The Audit Committee should support the Board and the Accounting Officer by reviewing the comprehensiveness of assurances in meeting the Board and Accounting Officer's assurance needs, and reviewing the reliability and integrity of these assurances.

Good Practice Questions

Terms of Reference	Yes	No	N/A
1 Have all executive responsibilities, and making or endorsing of decisions been excluded from the roles and responsibilities of the Audit Committee members?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2 Does the Audit Committee follow up recommendations regarding its effectiveness?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3 Does the Audit Committee's role include monitoring and reviewing the executive's processes for assessing, reporting and owning business risks and their financial implications?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4 Has the role and responsibilities of the Audit Committee been clearly defined and communicated to all Audit Committee members, along with details of how the Committee supports the Board?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5 Are the Terms of Reference reviewed at least annually by the Board and the Audit Committee, to ensure that the work of the Audit Committee is aligned with good practice and business needs?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6 Do the Terms of Reference include rules for a quorum?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7 Does the Audit Committee meet regularly (at least four times a year), and do meetings coincide with key dates in the financial reporting and audit cycle?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Additional Comments:**Conclusions**

Do we achieve **Principle 1: The Role of the Audit Committee** – Does the Audit Committee support effectively the Board and the Accounting Officer by reviewing the comprehensiveness of assurances to satisfy their needs, and by reviewing the reliability and integrity of these assurances?

What do we need to do to enhance the Audit Committee?

Where we have carried out the self-assessment before, the audit committee has improved its performance against:

- 1 none of the good practice questions.
 - 2 some of the good practice questions.
 - 3 most, if not all of the good practice questions.
-

Principle 2: Membership, Independence, Objectivity and Understanding

The Audit Committee should be independent and objective; in addition, each member should have a good understanding of the objectives and priorities of the organisation and of their role as an Audit Committee member.

Good Practice Questions

Independence		Yes	No	N/A
8	Is the Chair of the Audit Committee different from the Chair of the Board?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	Are the Audit Committee members either independent non-executive Board members or independent external members, and have they been appointed for an appropriate period of time (e.g. three years)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Relationship with the Executive				
10	Are the Executive members of the organisation invited to attend Audit Committee meetings, participate in discussions, and provide information to the Audit Committee as and when the Audit Committee deems it necessary?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other Participants				
11	Where appropriate, does a representative from the sponsoring body attend the Audit Committee meetings (e.g. if an Executive Agency, does a member of the Sponsoring Department attend the meeting)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	Does the Accounting Officer, Finance Director, Head of Internal Audit and the External Auditor routinely attend the Audit Committee, or attend at the request of the Audit Committee members?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	Are the numbers attending the Audit Committee meetings sufficient to deal adequately with the agenda, but not too many to blur issues?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Conflict of Interest				
14	Is the first agenda item of every meeting a request for the Audit Committee members to declare any potential conflict of interest with any of the business items on the Audit Committee's agenda?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Conflict of Interest (continued)		Yes	No	N/A
15	In instances where there is a declaration of interest in any of the agenda business items, are appropriate actions taken, e.g. is the member asked to leave the meeting while the business item is being discussed?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	In instances where the conflict of interest is likely to last for a long time, has the Audit Committee member been asked to relinquish his or her membership?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17	Are the Audit Committee members required to declare their interest in a register of interests?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Terms of Appointment				
18	Do all Audit Committee members have a clear understanding of what is expected of them in their role, set out in a letter of appointment, including:			
	a. their appointment and purpose;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b. the support and training that they will receive;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	c. the commitment required;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	d. their remuneration;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	e. conflict of interest procedures;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	f. expected conduct;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	g. duration of appointment and how often it may be renewed;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	h. how their individual performance will be appraised, including a clear understanding of what would be regarded as unsatisfactory performance; and	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	i. termination conditions?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Additional Comments:

Conclusions

Do we achieve **Principle 2: Membership, Independence, Objectivity and Understanding** – Is the Audit Committee suitably independent and objective, and does each member have a good understanding of the objectives, priorities and risks of the organisation, and of their role on the Audit Committee?

What do we need to do to enhance the Audit Committee?

Where we have carried out the self-assessment before, the audit committee has improved its performance against:

- 1 none of the good practice questions.
 - 2 some of the good practice questions.
 - 3 most, if not all of the good practice questions.
-

Principle 3: Skills

The Audit Committee should collectively possess an appropriate skills mix to perform its functions well.

Good Practice Questions

Range of Skills	Yes	No	N/A
19 Are there formal assessment criteria for the appointment of the Audit Chair, including attitudes to non-executives, strength of personality, experience of chairing, and time commitment?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20 Do the assessment criteria of Committee members include, or expect Audit Committee members to acquire as soon as possible after appointment:			
a. understanding of the objectives of the organisation and current significant issues for the organisation;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b. understanding of the organisation's structure, including key relationships such as that with a sponsoring department or major partner;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c. understanding of the organisation's culture;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
d. understanding of any relevant legislation or other rules governing the organisation; and	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
e. broad understanding of the government environment, particularly accountability structures and current major initiatives?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
21 Does the Audit Committee ensure that there are areas of collective understanding, including:			
a. accountancy – with at least one member having recent and relevant financial experience;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b. governance, assurance and risk management;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c. audit;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
d. technical or specialist issues pertinent to the organisation's business;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
e. experience of managing similar sized organisations;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
f. understanding of the wider environments in which the organisation operates; and	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
g. detailed understanding of the government environment and accountability structures?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Additional Skills		Yes	No	N/A
22	Do the Audit Committee members feel empowered to:			
a.	co-opt members for a period of less than one year to provide specialist skills that the members do not have to be an effective Committee;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b.	procure specialist advice at reasonable approved expense to the organisation, on an ad-hoc basis to support them in relation to particular pieces of Committee business.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Training and Development				
23	Is there an induction checklist for new Audit Committee members that details key things that they must do e.g. visits to important business locations, meetings with Board, Risk Manager, Internal Audit and External Auditors?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
24	Do all new members of the Audit Committee attend an induction training course for Audit Committee members run by the National School of Government, or other sector-related organisation?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
25	Does the Audit Committee ensure that new members have sufficient knowledge of the business to identify the key risk areas and to challenge both line management and internal and external auditors on critical and sensitive issues?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
26	Does the Audit Committee and the Chair make recommendations to the Board on the Committee's and individual members training needs?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
27	Does the Audit Committee keep abreast of best practice and developments in corporate governance in central government and more widely?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Additional Comments:**Conclusions**

Do we achieve **Principle 3: Skills** – Does the Audit Committee contain or have at its disposal an appropriate mix of skills to perform its functions well?

What do we need to do to enhance the Audit Committee?

Where we have carried out the self-assessment before, the audit committee has improved its performance against:

- 1 none of the good practice questions.
 - 2 some of the good practice questions.
 - 3 most, if not all of the good practice questions.
-

Principle 4: Scope of Work

The scope of the Audit Committee's work should be defined in its Terms of Reference, and encompass all the assurance needs of the Board and Accounting Officer. Within this, the Audit Committee should have particular engagement with the work of Internal Audit, the work of External Auditor, and Financial Reporting issues.

Good Practice Questions

Relationship with Internal Audit		Yes	No	N/A
28	Does the Audit Committee consider the independence and effectiveness of Internal Audit?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
29	Does the Audit Committee consider that the experience, expertise and professional standard of the Internal Audit team are appropriate for the size, complexity, and inherent risk of the organisation?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
30	Does the Audit Committee consider that the scope of Internal Audit work, the available resources at its disposal, and their access to information and people allow it to address significant risks within the organisation?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
31	Does the Audit Committee review and approve the Internal Audit plan before they commence any work and make suggestions regarding risk and problem areas that the audit could address in the short and long term?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
32	Does the Audit Committee receive regular progress reports on studies/work undertaken by Internal Audit?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
33	Does the Audit Committee review internal audit reports and management responses to issues raised, and monitor the progress made on Internal Audit's recommendations?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Relationship with External Audit				
34	Where relevant, does the Audit Committee consider the independence, objectivity, and effectiveness of the External Auditors?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
35	Does the Audit Committee periodically obtain the views of the External Auditor on the work and effectiveness of the Audit Committee?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Relationship with External Audit (continued)		Yes	No	N/A
36	Is the Audit Committee informed by the External Auditors on an annual basis as to their quality control procedures and compliance with applicable UK ethics guidance?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
37	Does the Audit Committee consider the External Auditor's Audit Strategy before they commence work, and make suggestions regarding risk and problem areas the audit could address in the short and long term?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
38	Do the External Auditors inform the Audit Committee of key developments and issues at key stages of the audit?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
39	Where relevant, does the Audit Committee review the audit fees?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
40	Does the Audit Committee consider the management letter and other relevant reports (e.g. the NAO's Value for Money work), and the management's response, and monitor the progress made on the recommendations?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Relationship between Internal Audit and External Auditors				
41	Does the Audit Committee consider whether there are areas where joint working between Internal Audit and the External Auditors would be beneficial?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
42	Does the Audit Committee seek confirmation from Internal Audit and the External Auditors on the effectiveness of the relationship?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fraud				
43	Does the Audit Committee consider whether effective anti-fraud and corruption policies and procedures are in place and operating effectively?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
44	Does the Audit Committee consider whether there is a code of conduct and its distribution to employees?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
45	Does the Audit Committee consider whether management arrangements for whistle-blowing are satisfactory?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Internal Control		Yes	No	N/A
46	Does the Audit Committee consider whether corporate governance is embedded throughout the organisation, rather than treated as a compliance exercise?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
47	Does the Audit Committee consider whether the system of internal reporting gives early warning of control failures and emerging risks?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
48	Does the Audit Committee consider whether the Governance Statement is sufficiently comprehensive and meaningful, and the evidence that underpins it?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
49	Does the Audit Committee satisfy itself that the system of internal control has operated effectively throughout the reporting period?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
50	Does the Audit Committee consider whether financial control, including the structure of delegations, enables the organisation to achieve its objectives and achieve good value for money?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
51	Does the Audit Committee monitor whether the organisation's procedures for identifying and managing business risk have regard for the relevant legislation and regulation?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Financial Reporting				
52	Does the Audit Committee review the first draft of the annual accounts before the External Auditors start work on them?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
53	Before the Accounting Officer signs off the Annual Report and Financial Statements, does the Audit Committee consider:			
	a. that the accounting policies in place comply with relevant requirements, particularly the Treasury's Financial Reporting Manual and Accounts Direction;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b. that there has been a robust process in preparing the accounts and annual report;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Financial Reporting (continued)		Yes	No	N/A
c.	whether the accounts and annual report have been subjected to sufficient review by management and by the Accounting Officer and/or Board;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
d.	that when new or novel accounting treatments arise, whether appropriate advice on accounting treatment has been taken;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
e.	whether there is an appropriate anti-fraud policy in place, and whether losses are suitably recorded;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
f.	whether suitable processes are in place to ensure accurate financial records are kept;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
g.	whether suitable processes are in place to ensure regularity and propriety is achieved; and	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
h.	whether issues raised by the External Auditors have been given appropriate attention.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
54	Where the accounts have been qualified, does the Audit Committee consider the action taken by the Board to deal with the causes of the qualification?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
55	Does the Audit Committee satisfy itself that the annual financial statements represent fairly the financial position of the organisation, regardless of the pressures on executive management?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
56	Before the Accounting Officer signs off the Letter of Representation, does the Audit Committee review it and give particular attention to non-standard issues of representation?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Additional Comments:

Conclusions

Do we achieve **Principle 4: Scope of Work** – Is the scope of the Audit Committee suitably defined, and does it encompass all the assurance needs of the Board and Accounting Officer?

What do we need to do to enhance the Audit Committee?

Where we have carried out the self-assessment before, the audit committee has improved its performance against:

- 1 none of the good practice questions.
 - 2 some of the good practice questions.
 - 3 most, if not all of the good practice questions.
-

Principle 5: Communication

The Audit Committee should ensure it has effective communication with the Board, the Head of Internal Audit, the External Auditor, and other stakeholders.

Good Practice Questions

Reporting to the Board		Yes	No	N/A
57	Does the Audit Committee send regular reports or provide oral updates to the Board that they review at their meetings?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
58	Does the Audit Committee provide an Annual Report to the Board, timed to support preparation of the Governance Statement?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
59	Does the Annual Report of the Audit Committee present the Committee's opinion about:			
a.	the comprehensiveness of assurances in meeting the Board and Accounting Officers needs;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b.	the reliability and integrity of these assurances;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c.	whether the assurance available is sufficient to support the Board and Accounting Officer in their decisions taken and their accountability obligations;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
d.	the implication of these assurances for the overall management of risk;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
e.	any issues the Audit Committee considers pertinent to the Governance Statement, and any long-term issues the Committee thinks the Board and/or Accounting Officer should give attention to;			
f.	financial reporting for the year;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
g.	the quality of both Internal and External Audit and their approach to their responsibilities; and	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
h.	the Audit Committee's view of its own effectiveness, including advice on ways in which it considers it needs to be strengthened or developed.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Additional Comments:

Conclusions

Do we achieve **Principle 5: Communication** – Does the Committee engage effectively with Financial and Performance Reporting issues, and with the work of internal and external audit? And does the Audit Committee communicate effectively with the Accounting Officer, the Board and other stakeholders?

What do we need to do to enhance the Audit Committee?

Where we have carried out the self-assessment before, the audit committee has improved its performance against:

- 1 none of the good practice questions.
 - 2 some of the good practice questions.
 - 3 most, if not all of the good practice questions.
-

Section II

The role of the Chair: good practice

The Chair of the Audit Committee has particular responsibility for ensuring that the work of the Audit Committee is effective, that the Committee is appropriately resourced, and that it is maintaining effective communication with stakeholders.

Good Practice Questions

Agenda Setting	Yes	No	N/A
60 Is the Board Secretary different from the Audit Committee Secretary?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
61 Does the Chair of the Audit Committee meet with the Committee Secretary before every meeting to discuss and agree the business for the meeting?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
62 Are inputs on Any Other Business formally requested in advance from Committee members and attendees?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
63 Are outline agendas planned one year ahead to cover core activities and specific issues on a cyclical basis?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
64 Does the agenda exclude executive business, so that there is no overlap with the work of the Board whilst linking to the main elements of the organisation's business?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
65 Are the meetings set for a length of time which allows all business to be conducted, yet not so long that the meeting becomes ineffective?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
66 Does the Chair encourage full and open discussion and invite questions at the Audit Committee meetings?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Communication			
67 Does the Chair of the Audit Committee have open lines of communication with the Board, Head of Internal Audit, and the External Auditors?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
68 Does the Chair encourage all Committee members to have regular interface with the organisation and its activities to help them understand the organisation, its objectives, and business needs and priorities?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
69 Do reports to the Audit Committee communicate relevant information at the right frequency, time, and in a format that is effective?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
70 Does the Audit Committee issue guidelines concerning the format and content of the papers to be presented to the Committee?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Yes	No	N/A
Monitoring Actions			
71 Does the Chair or the Secretariat ensure that all action points from Committee meetings are appropriately acted upon?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
72 Does the Chair or the Secretariat ensure that members who have missed a meeting are appropriately briefed on the business conducted in their absence?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
73 Is a report on matters arising made and minuted at the Audit Committee's next meeting?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appraisal	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
74 Does the Chair ensure that the Committee members are provided with an appropriate appraisal of their performance as a Committee member?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
75 Does the Audit Committee Chair seek appraisal of their personal performance from the Accounting Officer or Chair of the Board?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
76 Are Audit Committee meetings well attended, with records of attendance maintained and reviewed annually by the Board?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appointments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
77 Is the Chair involved in the appointment of new Committee members, including providing advice on the skills and experience required of the new individual?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Additional Comments:**Conclusions**

Do we meet **Good Practice: the Role of the Chair** – Is the Committee appropriately resourced, work planned in advance as far as possible, and effective communication with stakeholders maintained?

What do we need to do to enhance the Audit Committee?

Where we have carried out the self-assessment before, the audit committee has improved its performance against:

- 1 none of the good practice questions.
 - 2 some of the good practice questions.
 - 3 most, if not all of the good practice questions.
-

Section III

Committee support: good practice

The Audit Committee should be provided with appropriate Secretariat support to enable it to be effective. This is more than a minute-taking function – it involves providing proactive support for the work of the Committee, and helping its members to be effective in their role.

Good Practice Questions

Does the Audit Committee Secretariat:	Yes	No	N/A
78 Commission papers as necessary to support agenda items?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
79 Circulate meeting documents to all Committee members, Internal Audit and External Auditors in good time before each meeting, to allow members time to study and understand the information e.g. at least one week before the meeting?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
80 Arrange for Executives/senior management to be available as necessary to discuss specific agenda items with the Audit Committee during meetings?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
81 Keep records of meetings and minutes after they have been approved by the Audit Chair and circulate them to Committee members, Head of Internal Audit, External Auditors, Board, and the Accounting Officer on a timely basis e.g. within one week of the meeting?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
82 Ask for confirmation that the minutes are a true and fair representation of a summary of the business taken by the Audit Committee?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
83 Ensure that the minutes clearly state all agreed actions, the responsible owner, when they will be done by and any advice given from any stakeholders?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Does the Audit Committee Secretariat: (continued)		Yes	No	N/A
84	Ensure action points are being taken forward between meetings?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
85	Support the Chair in the preparation of Audit Committee reports to the Board?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
86	Arrange the Chair's bilateral meetings with:			
	a. the Accounting Officer, the Head of Internal Audit, Director of the External Auditors;	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b. the Chair of the Board of sponsored NDPBs.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
87	Keep the Chair and members in touch with developments and relevant background information about developments in the organisation?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
88	Maintain a record of when members' terms of appointment are due for renewal or termination?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
89	Ensure that appropriate appointment processes are initiated when required?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Additional Comments:

Conclusions

Do we meet **Good Practice: Support for the Committee** – Does the Committee receive appropriate support from its secretariat?

What do we need to do to enhance the Audit Committee?

Where we have carried out the self-assessment before, the audit committee has improved its performance against:

- 1 none of the good practice questions.
 - 2 some of the good practice questions.
 - 3 most, if not all of the good practice questions.
-

Where to find out more

The National Audit Office website is

www.nao.org.uk

Links to other websites

www.hm-treasury.gov.uk/audit_committee_handbook.htm

www.hm-treasury.gov.uk/d/mpm_annex3.1.pdf

If you would like to know more about
the NAO's work in this area please email

Z5-FMGP@nao.gsi.gov.uk

www.nao.org.uk/financial-management

Twitter: [@NAOorguk](https://twitter.com/NAOorguk)

Sign-up to NAO direct: www.nao.org.uk/NAOdirect

Design & Production by
NAO Communications
DP Ref: 009797-001

© National Audit Office | January 2012
First published in 2009



www.nao.org.uk

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 17

Paper number AGC (07/12/2016) 522

Meeting date 7 December 2016

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
High Level Risk Register	Yes	Yes	Yes	Yes
Information for Quality (IfQ) Prog	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	Results, annual opinion approve draft plan	Update	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
HR, People Planning & Processes		Yes		

AGC Items Date:	21 Mar 2017	13 Jun 2017	3 Oct 2017	5 Dec 2017
Strategy & Corporate Affairs management			Yes	
Regulatory & Register management				Yes
Resilience & Business Continuity Management				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				