Information for Quality (IfQ) Programme – Data Migration

Strategic delivery:	☐ Setting standards	☐ Increasing and informing choice	☒ Demonstrating efficiency economy and value
Details:			
Meeting	AGC		
Agenda item	6		
Paper number	HFEA (15/06/2016) 497		
Meeting date	15 June 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 – programme timeline Annex B – Digital service Assessment			

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 has now reached the closing stages of the Beta phase and we are preparing to launch both the new Website and Clinic Portal to 'public beta'.

1.2. After successfully passing the May assessment against the Government Digital Service (GDS) standards by the Department of Health (DH), the team is focused on addressing the resulting recommendations prior to completing 'public beta' and subsequently putting release 1 of the services to full 'live'.

1.3. Annex A sets out the timeline for the remaining IfQ Beta phase, leading both to 'live' and to the next DH/GDS assessment.

2. IfQ projects update

2.1. IfQ DH/GDS assessment

- Since the last report, the IfQ team has achieved a significant milestone on our journey to releasing the HFEA's new Website and Clinic Portal to 'public beta'.
- On 11 and 12 May, the Department of Health conducted a full review of the new Website and Clinic Portal against the 18 Government Digital Service Standards, to assess the readiness of both services to proceed to 'public beta'.
- We are pleased to report that both products passed this assessment, which serves as a welcome endorsement of the work of the IfQ Programme team to date.
- As with any useful review process, our pass came with some recommendations, and activity to address those will now be incorporated alongside our other priorities during each 'sprint' (see annex B). The associated GDS spend control approval process to release planned budget to be spent on preparing for full release 1 'live' and release 2 development is now underway.

2.2. IfQ private and public beta – website and clinic portal

- Having been granted permission to do so, the next important step for the programme team is to now go ahead and transition the service from development to 'public beta', which is to make the website and portal available to real end users.
    - **For both the new HFEA website and the new Clinic Portal, the services will be put to public beta on 29 June 2016**.

      For the first two weeks, only clinics will have access to the new HFEA website, in order to provide them with some time to view the new content and statistics that relate to them on their CaFC Profiles. After this two-week period, the new HFEA website will then be made available to the broader public.
- We are currently anticipating that public beta for both the portal and the website will run for a period of approximately 10 weeks.
- This may change, subject to what we learn during public beta. For example, if users indicate that there are significant changes required, we can extend the length of public beta. Alternatively, if there are limited changes required, or approvals are received quickly, we may require less time.

- After public beta, release 1 of IfQ will then be transitioned to a full 'live' service. This step requires both the website and clinic portal services to pass another full gateway assessment by the Department of Health against the 18 Government digital standards.

2.3. Planning for 'Release 2'

- The IfQ Programme team is now finalising all planning activity for the next significant milestone in the programme – 'release 2' that is the replacement for EDI and the new Register. This follows a review and refinement of all requirements. This detail is being utilised to inform the order of priority for building the key features of release 2, which will be incorporated in IfQ's overall delivery plan.
- In line with the programme's delivery plan, foundational work on the internal infrastructure and architecture required to support release 2 has commenced.

2.4. IfQ data cleansing

- The Register Information team is working with centres currently on 'severity 1 errors' - initially by way of a 'pilot.' There were only 63 errors being addressed in the first tranche of eight centres. We are now following up with a further 18 centres. The process is being managed carefully so as to ensure that our staff are available to field queries from the centres and to assist them where necessary.
- There are currently a total of 3500 severity 1 errors to be reviewed prior to the data migration. 1240 errors have been fixed across all centres during the last period of cleansing – demonstrating reasonable progress.
- Centres who have fixed all their severity 1 errors will be sent additional severity 2 errors to keep the momentum, and cleanse as much as possible data prior the data migration. Also note that severity 2 cleansing is not an impediment for the data migration process.
- The differences between the draft data dictionary and the proposed new Register structure are being discussed by the project team. These discussions will ensure that the final published data dictionary will properly match the underlying new data structure.

3. Update on data migration process

3.1. Background on the revised Register of treatments

- As AGC members are aware, IfQ involves important changes to the way we collect, use and publish information. Critically, this work will involve significant changes to the HFEA's 'Register of Treatments' (the Register).

- The Register holds information about people receiving fertility treatment, egg and sperm donors, and children conceived following treatment. Keeping the Register is one of the HFEA's statutory obligations and the information currently held in the Register is likely the largest database of assisted reproductive treatments in the world. The Register is critically important for a number of reasons:

    - As a comprehensive record of all treatments, it provides crucial information on the safety and effectiveness of treatments
    - It enables donor conceived people to have knowledge of their genetic inheritance
    - It enables parents to access information about the donor used in their treatment
    - It enables donors to understand the outcome of their donation
    - It enables patients to make more informed choices about their treatment options
    - It supports intelligent regulation and makes possible important research and analysis.

- A key outcome of IfQ will be changing what information is kept in the Register, how that data is recorded and how it is collected or obtained. To achieve this, we have carried out a review to ensure each item of data collected from clinics is fully justified, and subsequently determined a new draft dataset that should be collected from clinics.

- Based on this new dataset, we are creating a revised Register, which will use modern database practices and technology. Improvements to the way that data is recorded and stored in the revised Register will result in higher quality data, which is more accessible to us and to other key stakeholders and interest groups – such as researchers.

- In addition, the revised Register will work hand in hand with the replacement for EDI to meet key investment objectives for IfQ by reducing the administrative burden for clinic users.

3.2. Data migration process and strategy

- The revised Register must be populated with data, requiring the transfer of historic information from the existing Register database in to the new Register database structure. This is referred to as the IfQ 'data migration' process. This process is related, though different to, the 'data cleansing' process, which seeks to improve the quality of historical data being transferred to the revised Register.

- Due to the importance of the Register and the highly sensitive nature of the data contained within it, a well-managed and successful data migration process is central to realising many of the anticipated benefits of the IfQ Programme. At its last meeting AGC requested a more in-depth report on progress to date.

- In recognition of the importance of the data migration process, external suppliers 'Avoca' were engaged to provide their expertise and work with us to develop a strategy for completing the data migration process appropriately. That strategy was reviewed and accepted by the HFEA in March 2015, and has been used to inform each key step of the migration process since.

- The strategy required a foundational ‘health check’ of the data to be conducted, which identifies data quality issues at the outset of the project, to guide realistic project planning and risk mitigation activities. This Health Check was completed in late 2015, with the results presented to the IfQ Programme Board.

- Following the health check of the data, the strategy requires five separate data migration ‘loads’ of all of the historical data in to the new Register structure. The first four are ‘trial loads’ in preparation for the fifth and final load. To ensure that an appropriate level of testing, quality control and assurance has been carried out before the fifth and final load, the following key processes are undertaken within each prior load:

    - **Interim File Format (IFF) mapping report:** provides an overview of how well Register data will ‘fit’ into the new Register database, including visibility of a variety of scenarios that require further attention.

    - **Code set mapping report:** indicates how well the new Register can be populated using the actual data values present in the current Register, again including various scenarios requiring further attention.

    - **Mapping and rules document:** contains detailed but plain-English descriptions of how each and every field in the new Register will be populated, including all cleansing (corrective) rules to be applied as well as data transformations to suit the new Register’s different structure.

    - **Reconciliation report:** audits the quantities of data in the current Register against what was migrated to the new Register during a trial load, to prove that no data has been lost unless this has been agreed by all stakeholders.

    - **Migration exceptions report:** gives management visibility of errors or problems encountered with a trial data load, so issue resolutions can be tracked over time.

    - **Approval to proceed document:** summarises outstanding tasks for data quality improvement, to be carried forward into subsequent stages of the migration.

- In reality, there are many more than only five loads, with each trial load phase including a series of data loads to evaluate errors and problems as they are addressed incrementally.

3.3. Timeline for data migration

- Currently, the Programme is progressing through trial load 1, having now produced each of the above reports and documents and having conducted several incremental trial loads. The team is currently finalising the reconciliation and migration exceptions reports in the lead up to commencing trial load 2.

- Trial load 1 was scheduled to be completed by 17 May 2016. Due to pressures on the internal systems team associated with completing the beta phase of the new website and clinic portal, we anticipate trial load 1 will be fully completed by 28 June 2016. Notwithstanding this delay, the team still anticipates being ready to complete trial load 5 by the end of September, in line with the current delivery plan for IfQ.

- This confidence is based on trial load 1 requiring each process to be conducted for the first time. The process will become significantly less burdensome as we progress through each subsequent trial load phase. Further, to account for this risk there was a large contingency built in to the timeframe for trial load 5, which will be partially consumed.

- Current timelines for the Data Migration process:

Programme milestone	Planned completion date	Anticipated completion date
Trial load 1	17 May 2016	28 June 2016
Trial load 2	28 June 2016	13 July 2016
Trial load 3	13 July 2016	28 July 2016
Trial load 4	28 July 2016	12 August 2016
Trial load 5	21 September 2016	21 September 2016

3.4. Data migration strategy assurance

- Regrettably, 'Avoca', the external supplier who produced the data migration strategy, has since gone out of business. This leaves unmet an important assurance role that we were anticipating Avoca would provide.

- Accordingly, we are currently in discussion with service providers and recruitment agencies, and we expect to finalise a procurement round before the end of June 2016, securing assurance services from another adequately qualified service provider. This will provide external assurance that we are completing the steps required in the data migration strategy, to the appropriate level of quality.

- In addition, the data migration activity has been subject to a number of internal audit reviews. The finding of each internal audit review have been considered by the IfQ Programme Board, and incorporated in to our ongoing assurance management log. Primarily, the key recommendations from those reviews have focused on adherence to the data migration strategy outlined above and managing the risk of balancing timely delivery of data migration against maintaining an adequate level of data quality as a result of data cleansing activity.

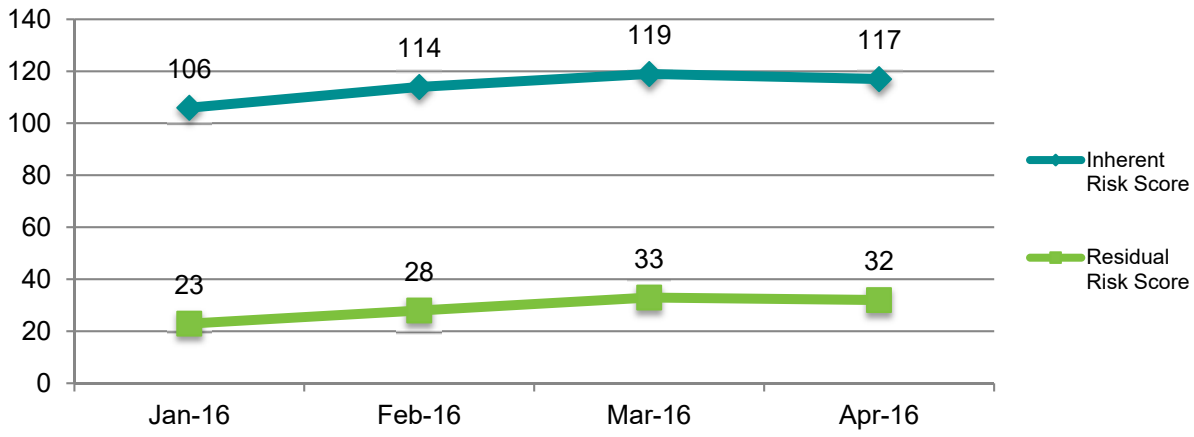
3.5. Safeguards

- Throughout the entire data migration process and when the new Register structure is operational, the existing Register database will be retained as a reference. This will ensure that there is no risk that the data migration activity compromises the actual data held in the current Register structure.

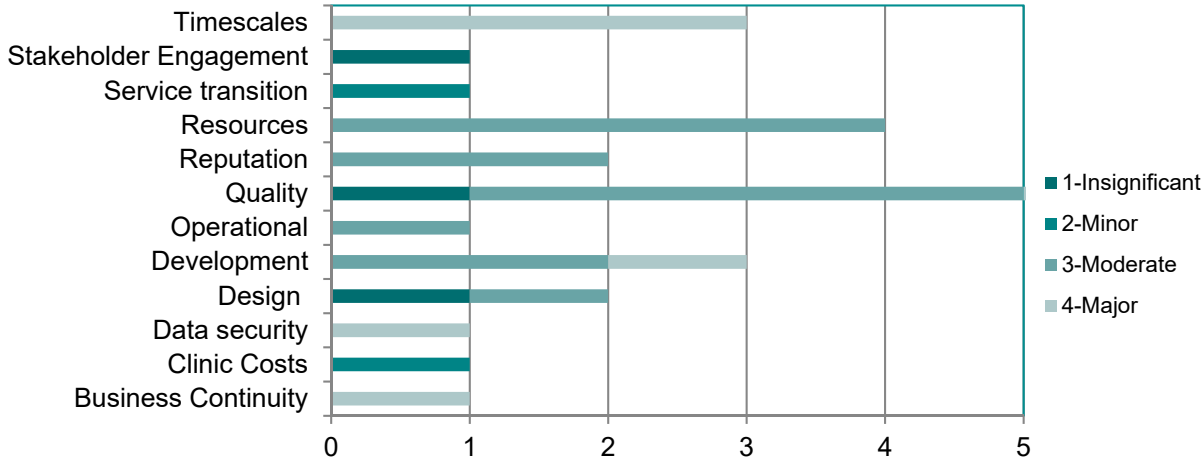
- As defined above, a reconciliation report will be produced during each trial load to identify where data has not been transferred in a usable way, according to the quality standards and technical structure of the new Register. This will ensure the HFEA knows exactly what data has been transferred successfully. In addition, data that doesn't meet these quality metrics will be 'flagged' in the new structure, to ensure it will be addressed, and as stated above, retained in the reference copy of the current Register for information.

4. IfQ risks and issues

- The below line graph represents the overall IfQ risk score, which combines the perceived impact and likelihood of the current risks each month. The overall risk score for the IfQ programme has slightly decreased since March 2016.



- The below bar graph shows the number of risks in the top 12 risk categories, coloured according to severity of risk. It shows that the greatest number of risks are contained in the quality, resources, timescales and development risk categories. The most severe risks are associated with timescales, development, data security and business continuity.



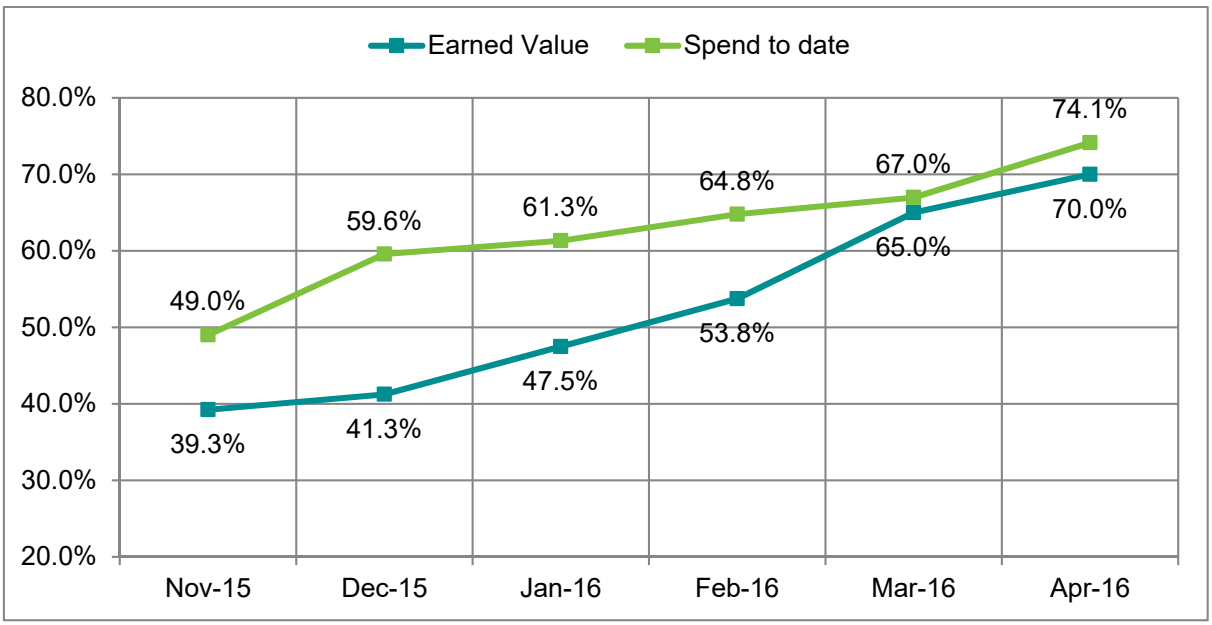
5. IfQ budget

- At the end of the 2015/16 financial year it was necessary to carry over £467k to the new financial year.
- Despite the underspend the total programme budget remains broadly on track across the 2015/16 and 2016/17 financial years.
- On 24 May 2016, SMT decided to allocate an additional (and new) £90k to the overall Programme budget to ensure that critical staff are retained on the team as the transition from delivering release 1 to release 2 is made. This modest additional investment essentially means we can continue working at pace but sharing the load so as not to burden key staff disproportionately.

6. Earned value

- The earned value and spend to date are converging. We are expecting the spending figures to increase in the upcoming month, due to receiving the beta invoices from Reading Room and also payment of external contractors who have started the work on security/CLAS needed for the internal systems project.
- There is a slight caveat to this, in that the percentage increase in the earned value measures the work under way for delivery of the project, rather than against the Agile 'definition of done' assessment. For April the main focus was on fixing bugs in existing work so as to ensure readiness for the GDS assessment. This was important work, but it meant that the proportionate level of new delivery underway was actually less than in previous months.

Period	Nov-15	Dec-15	Jan-16	Feb-16	Mar-16	Apr-16
Earned Value	39.3%	41.3%	47.5%	53.8%	65.5%	70.0%
Spend to date	49.0%	59.6%	61.3%	64.8%	67.0%	74.1%



7. Recommendation:

7.1. The Audit and Governance Committee is asked to:

- Note progress, risks and the budget position on IfQ
- Note in particular the update on the data migration process.

8. Annexes:

- Annex A: Timeline for the remaining IfQ Beta phase
- Annex B: Health digital service assessment Website and Clinic Portal

Programme Plan

15/6: Data shared with clinics in excel via CF and CE letter

29/6: Live CaFC site shared with clinics/stakeholders

10/8: Website User testing

17/8: Portal User testing

7/9: Website & Portal assessment

5/10: Website & Portal (R1) LIVE

	Sprint 11	Sprint 12	Sprint 13	Sprint 14	Sprint 15	Sprint 16	Sprint 17	Sprint 18	Sprint 19	Sprint 20
	18/5 – 31/5	1/6 – 14/6	15/6 – 28/6	29/6 – 12/7	13/7 – 26/7	27/7-9/8	10/8 – 23/8	24/8 – 6/9	7/9 – 20/9	21/9 – 4/10
Website	PREPARE FOR PUBLIC BETA (6 WEEKS)			CLINIC PUBLIC BETA (2 WEEKS)	PUBLIC BETA (8 WEEKS)				GDS APPROVAL & FURTHER TWEAKS (4 WEEKS)	
Clinic Portal	PREPARE FOR PUBLIC BETA (6 WEEKS)	EARLY ADOPTERS BETA		ALL CLINICS PUBLIC BETA (2 WEEKS)	PUBLIC BETA (8 WEEKS)				GDS APPROVAL & FURTHER TWEAKS (4 WEEKS)	

Health digital service assessment

HFEA website and clinic finder tool

The HFEA website provides information for patients, donors, donor-conceived people, professionals working in clinics, researchers and the media. The redesign project aims to better meet user needs and upgrade an outdated infrastructure.

The clinic finder is a tool for patients and clinics to get impartial, unbiased information about clinics, the treatments they offer and how successful they are. The redesign project aims to give users a greater understanding of treatments and data.

Department / Agency	Human Embryology and Fertility Authority (HFEA)
Date of assessment	11th May 2016
Assessment stage	Beta
Lead assessor	Matt Harrington (DH)
Result of assessment	Pass
Assessors	Dan Sheldon, Olga Passet , Lauren McAllister
Service manager	Trisram Dawahoo
Digital leader	Adam Bye

Assessment report

The HFEA website and clinic finder has been reviewed against the 18 points of the Service Standard at the end of beta development.

Outcome of service assessment

After consideration, the assessment panel has concluded that the HFEA website and find a clinic tool is on track to meet the Digital by Default Service Standard at this stage of development.

The panel would like to thank the service team for their time, the amount of effort which clearly went into the assessment and congratulate them on passing.

There are however, a number of recommendations which the team are now expected to address. Similarly, there is concern that an 8 week public beta may be too ambitious a time frame to truly learn about users and validate the decisions that have been made. The team should look to do the maximum amount of user research they can.

Reasons

User needs and assisted digital:
The assessment panel were pleased with the approach to user research by the team and the work they have done since alpha. It is clear that user needs are core to the development work and it was good to see how the team have taken steps to understand user groups and personas.

The team have taken steps to engage with assisted digital users as part of their research which is positive and this should be continued through beta to continue to develop this understanding.

It was good to hear the service manager and team talk passionately about working with users and give examples of learnings from user research. There is a plan for testing during beta and it puts the team in a good place where they will be able to learn even more with quantitative data.

The team:
The team appears to be working well and there are clearly defined roles for most positions you would expect within an agile team. As per the recommendations from Alpha, the team have brought in more content support in the form of a copywriter. It would be good to build relationships with the cross-government content design community and for the copywriter to avail themselves of any training and development opportunities provided in that network.

The team are continuing to work in agile, running two week sprints with sprint artefacts. The team use show and tells to communicate their work to the wider organisation and are using a backlog to manage the work and prioritise development. The team have also set up a physical wall to better communicate the team's priorities and what everyone is working on.

Certain roles in the team are currently filled by a supplier, this seems to be working well and it is positive that the team is co-located. There is skill transfer happening and this will be particularly important in the future when the supplier contract ends.

Improving the service and design:
It was positive to see that the team have changed the service significantly since the Alpha assessment based on their user research. At the assessment we discussed further opportunities for testing and the team were keen to try these out.

The team still have challenges ahead, particularly in relation to displaying complex data. The work gone into this so far has been positive and the team understand the real user need. However, the team may benefit from stepping back and working with colleagues to see how else they could display complex data.

Security, privacy, tools and standards:

There is only one part of the service that captures data from users - the proposed comment facility at the bottom of some pages. Although this facility is subject to pre-moderation, the team should consider how to capture and store data that could be personal or sensitive. The

team should review whether this feature is necessary, or whether there are alternative ways to meet the same objective.

The team have chosen a technology stack aligned to their in-house skills. The team were aware of the risks of lock-in, and are confident their choice of technology will give them enough flexibility to iterate the service. The team should be wary of doing too much closely coupled customisation to Umbraco, as this will make future upgrades and changes harder.

The team are planning to open source their code when the service is live. The team should start to code in the open rather than waiting to the end to release code, ensuring any sensitive text (e.g. passwords) are kept in separate files and not shared in public repositories.

Although the team have an aspiration to open up clinic data, the plans are not clear. The team have not yet engaged with GDS to discuss registers.

Analysis and benchmarking:
The team already get data from an existing live service and have recently got a net promoter score to help act as a baseline for the future service. In addition to this, the team are going to add analytics ready for beta so that data can be collected from the outset. Retesting the new site to see change in net promoter score will provide some insight but shouldn't be the only measure.

The team are expecting to use the in-page rating and commenting tool to enable them to iterate based on user feedback. It is positive to see they are keen to do this, but should consider all options available to get direct user feedback.

It was particularly pleasing to hear that the team are already considering KPIs for public beta to measure hypotheses, these will be good to show at the live assessment.

Testing with the Minister

The team have engaged their Chief Executive who has seen the service which is positive, they should however put a plan in place to test with the minister to showcase their work.

Recommendations:

Before public beta:

- Resolve Javascript issues prior to public beta launch to ensure the website works fully without Javascript capability.

User needs and assisted digital:

- Develop a plan, and conduct user research to integrate qualitative research with the incoming google analytics data.
- Run a heuristic analysis of the interface design elements with focus on usability, interactive elements and design language consistency.

- Have a way to measure the success of the assisted digital support through the beta period.

The team:

- The work doesn't stop after public beta. The team need to establish a plan for the continued development of the service once the current delivery partner leaves.

Improving the service and design:

- Take time to review against the service manual and design patterns. Some of this has been done, but there are more opportunities to improve the service. (Additional design comments sent via email)
- Review the possibilities of integrating iconographic elements to increase the recognisability of information fields and improve the overall UX (something that could be tested with A/B tests).
- Test different designs of the clinic search to see whether efficiency could be improved, e.g. one line of information per clinic to make comparison easier, advanced filtering appearing later in the journey etc.
- Review and improve the user journey for donors.
- Review search functionality as it is currently confusing and consider/test a universal search function.
- Review the need for a published comment facility at the bottom of content pages. Investigate alternatives (e.g. a GOV.UK style simple feedback mechanism)

Security, privacy, tools and standards:

- Provide the list of clinics as a public register via an API and variety of different standard representations.
- Engage with Paul Downey at GDS to discuss the cross-government registers work, and reuse the code or build their register to the standards GDS are setting.
- Work closely with NHS Choices to provide the clinic data to their service finder.
- Review privacy impacts of comment facility.
- Start to code in the open.

Summary:

The team have made great progress and done well continuing to iterate the website and clinic finder since the alpha assessment. The team have it within their ability to build a user focused service and a public beta will provide them with qualitative data to go alongside their user research to continue to build and iterate.

Digital by Default Service Standard criteria

Criteria	Passed	Criteria	Passed
1	Yes	2	Yes
3	Yes	4	Yes
5	Yes	6	Yes

7	Yes	8	Yes
9	Yes	10	Yes
11	Yes	12	Yes
13	Yes	14	Yes
15	Yes	16	Yes
17	Yes	18	Yes

Health Digital Service Assessment

HFEA clinic portal

The clinic portal allows clinics to submit, obtain and manage clinic information and allows HFEA to give clinics performance data. Clinics will access alerts, guidance and news via the portal. Inspection reports and other compliance activities will be published here.

HFEA are redesigning the clinic portal to combine existing and enhanced functionality and make it easier to use by: improve the quality of data submitted to HFEA; reduce the “burden” associated with data submission; provide added utility; provide an improved user experience of accessing information and submitting data.

Department / Agency:□	Human Embryology and Fertility Authority (HFEA)
Date of Assessment:	12 May 2016
Date of Original Assessment:	N/A
Assessment Stage:□	Public Beta
Lead Assessor:□	L. Scott
Result of Assessment:	Pass
Assessors:	A. Davidson, O. Passet
Service Manager:□	Chris Hall
Digital Leader:	Adam Bye

Assessment report

The HFEA clinic portal has been reviewed against the 18 points of the Service Standard at the end of the beta development.

Outcome of service assessment

After careful consideration the assessment panel has concluded that on balance, the clinic portal service is on track to meet the Digital by Default Service Standard at this mid stage of development, and can proceed into public beta.

The panel would like to thank the service team for their time, the amount of effort which clearly went into the assessment and congratulate them on passing.

There are however, a number of recommendations which the team are now expected to

address. Similarly, there is concern that an 8 week public beta may be too ambitious a time frame to address these recommendations and remain on track to progress to a live service.

Reasons

The service was assessed against all 18 points of the Digital by Default Service Standard. We asked questions from the prompts and evidence for assessors, supplied by GDS. This document has questions and the evidence sought for alpha, beta and live phases. We asked questions from the beta section.

On balance, the service currently meets the requirements of the standard for an beta service. The comments below reflect some of the observations we made during the discussion. Recommendations are listed later in this report.

The service team must address the recommendations made, course-correcting development where necessary, to ensure that the project remains on track and adheres to the service standard as it moves through the next phase.

User needs and assisted digital

The team have carried out 1:1 research sessions with a regional spread. These were recorded and the service manager observed some. The development team works closely with the user researcher to gain insights. The usability sessions were task-led, prompted by user needs uncovered in earlier research. Although the information architecture has been iterated following research, it wasn't a user-led design from the start.

The service manager also meets regularly with stakeholder and expert groups, demonstrating the prototype and gathering feedback.

The team have amassed learnings about users during development, and could demonstrate knowledge about the types of users they had, and contextual information about them. They pointed to where their assumptions has been challenged, eg around the 'person responsible' being the sole user.

Although the team get updates from the user researcher and have access to the reports, they should be taking the opportunity to accompany the researcher and get exposure to users in the field. The public beta is a perfect opportunity for the whole team to visit clinics and observe users trying out the service. Developers and designers will benefit from seeing research first hand, being able to use their knowledge of the software to suggest better functionality to meet needs.

We spent some time discussing the Knowledge Base part of the service. This is a core user need - finding guidance from HFEA. Expert view (backed up by the service team's research) shows that this needs significant iteration to meet user needs. The important information takes a lot of scrolling to get there. It looked like this part of the service was being used to broadcast corporate messages as well as meeting user needs, with the former taking priority.

The To Do List also addresses a big problem users experience now re: tracking outstanding actions with HFEA. It's tested well, though the panel found the interplay of 'status' and 'priority' confusing.

The design of the performance dashboard may look like data visualisation rather than formatting. We discussed ways of mitigating this.

The team have not found any users with any assisted digital needs. They plan to ensure this is the case during public beta. There is a support centre in place, accessed via telephone, if people need help accessing the digital service.

The team plan to carry further rounds of lab testing in public beta.

The team

Most of the deep digital roles are provided by the supplier. Some skills transfer is taking place. Independent contractors are also skilling up the in-house IT team to ensure they can support the service. Great to see the service manager taking an active role in user research - although professional skills should still be sought to ensure that methodologies, best practice etc is being applied. Service manager, content and delivery manager skills are in-house. This set up will continue during public beta. The team should make plans now for continuous improvement of the live service, factoring in costs for buying in expert skills, as that looks likely to still be necessary.

The team are using agile techniques to plan work and seem content and comfortable with agile artefacts. Great to hear examples of agile being applied at a more strategic level - eg the roadmap has completely changed from a year ago, due to learnings from research and experimentation.

Security, privacy, tools and standards

The team are planning to open source their code when the service is live. The team should start to code in the open now rather than waiting to the end to release code, ensuring any sensitive text (e.g. passwords) are kept separately and not shared in public repositories (for instance, in an associated private repository, or a secrets-management service).

The team currently have a commendably agile approach to deployment, with code being automatically deployed as soon as tests have been successfully performed. However, the panel is concerned that they are planning to be less agile in future, by "bundling up" changes to be released in the middle of the night or potentially at the end of a sprint. We recommend that they instead maintain their current process and focus their effort on minimising the user impact of a release through, for instance, parallel-stack/dns-switching deployment.

The technical architecture of the service appears rather over-engineered for the current stage and expected load on the service, even once fully rolled-out. Whilst the panel recognise that future storage of patient-identifying data may result in some data-separation requirements, we

believe that a simpler architecture may have allowed the team to deliver user benefits earlier, and would encourage an 'emergent architecture' approach.

The team have clearly done some thinking around security threats and potential for fraud, and are engaging with appropriate risk owners. We recommend that for future assessments the team provide evidence of this thinking in a short document, listing potential threats alongside their likelihood and potential impact, and actions they have taken to mitigate each threat.

Design

Although the service is exempt from the visual look and feel of GOV.UK, the GDS design patterns still stand as an accepted starting point for evidenced best practice in service design and user interaction standards.

Again, the GDS content style guide should be used as starting point for patterns (even if the service is exempt from technical style guide adherence) as to how users will successfully engage with a government service.

We couldn't see evidence that the team have adopted the design patterns or the content style guide as a starting point, despite a recommendation after alpha development. We did discuss the issue of accordions, which the team had considered, and we reiterate the point that the patterns are a starting base and the adoption should be 'consistent not uniform'.

Analysis and benchmarking

The team continue to mostly rely on user research to gather evidence for user needs and test concepts. Service teams should be making more use of data and analytics at this stage of development. There was still no evidence that the team had considered service metrics in any depth. Google Analytics will be instrumented during public beta. The team need a plan to make sure they are gathering meaningful data, analysing it and using this evidence to inform improvements.

There is no offline competing channel. Digital take-up targets are therefore 100%.

The team cited evidence from research that their users expect and desire to use a fully digital service.

Testing with the Minister

The team have engaged their Chief Executive who has seen the service. They have no plans as yet with the current minister with portfolio for this area, and do not know who this is.

Recommendations

User needs and assisted digital

1. The whole team needs to be involved in ongoing user research, including the development team at the supplier. Take the opportunity to go and observe users in context using the service in public beta.
2. Put thought into finding ways to make the navigational paths for your everyday power users more efficient.
3. Collect feedback on how personalisation (saving favourite documents, put together your own dashboard, etc.) can support your users.
4. Ensure the icons and the labelling in the ToDo list are understood by the users - gather evidence to demonstrate this.
5. Data and numbers are needed to justify design decisions made - ensure you use this kind of evidence to back up user research observations.
6. Ensure you have a way of collecting feedback (a banner could be an option) from users who view the beta service.
7. Don't forget to make use of the personas and update them if necessary.

The team

1. Establish a plan for continued development and a managed service once the current delivery partner leaves.
2. Ensure you have funding for and access to specialist roles in future. For example, user research. Whilst it's great the team is learning some of the principles and practices, expert help will be needed when using research to make service design decisions.

Technology, security and standards

1. Keep the current deployment automation in place.
2. Increase test coverage - 50% is acceptable for the current stage - it will not be for a live service.
3. Introduce explicit regression testing and smoke-testing for releases.
4. Keep in mind the danger of over-engineering for requirements which do not need to be accounted for yet.
5. Produce a document of risks considered, likelihood and impact of threat, and what mitigation is in place
6. Make code open now, and code in the open from now on.
7. Get analytics data on browsers and devices and design accordingly.
8. Produce an explicit plan for disaster recovery.
9. Consider a fallback offsite backup facility. Regularly test both local and offsite backups.

Design and content

1. Test and measure whether users understand the meaning of certain words and acronyms (red, green status...)
2. Plan for how to improve the interaction design as you gather more evidence during beta when you'll get a higher volume of users.
3. Review the order of the navigational elements against evidenced user needs.
4. Obtain data and evidence on what browsers and devices your users are using, and design accordingly. Analytics from the existing service may help here.
5. Run a heuristic analysis of the interface design elements with focus on usability, interactive elements and design language consistency against the GDS design patterns.
6. Resolve Javascript issues prior to public beta launch. Currently the service requires Javascript for some critical things - e.g. viewing what's required on a to-do list.
7. Check that the capitalisation is in sentence case style consistently across the site and avoid using full caps for anything apart from acronyms.
8. Ensure that the responsive design actually works on mobile devices: eg the burger menu doesn't work in Chrome on a smaller screen without a refresh.
9. Consider testing a more appropriate way of visualising percentages and other data on the dashboard.

Analysis and benchmarking

1. Work out a plan for measuring the service against the 4 mandated KPIs (where these are relevant). Communicate this.
2. Plan to collect, analyse and act on any other meaningful metrics that will whether the service is making things better.

Testing with the Minister

1. Identify the Minister with portfolio for this area and make plans to demonstrate the service.

Summary

The cross-government panel really appreciated the honesty and clarity of the responses - this helped us assess the service against the standard. Great to see significant progress made since the alpha assessment. It's excellent to see a multidisciplinary team working together to deliver this service. By taking the steers outline above, the service team will be making sure that the standard is adhered to throughout the next stage of development, resulting in a service that is user led, safe and secure, and easily improved.

Digital by Default Service Standard criteria

Criteria	Passed	Criteria	Passed
1	Yes	2	Yes

3	Yes	4	Yes
5	Yes	6	Yes
7	Yes	8	No
9	Yes	10	No
11	Yes	12	Yes
13	Yes	14	Yes
15	No	16	No
17	Yes	18	No

ANNUAL ASSURANCE REPORT 2015/16

Human Fertilisation and Embryology Authority

Health Group Internal Audit Service

Background

In order to be able to provide an annual opinion for 2015/16 to the Human Fertilisation and Embryology Authority's (HFEA) Accounting Officer, it is necessary to consider the work undertaken by Internal Audit over the course of the year, the outcomes of that work and feedback from management on improvements to their areas of responsibility as a result of that work. This together with wider intelligence gathered from all sources of assurance (including the NAO) and performance reporting, inform the Head of Internal Audit's view of controls, governance and risk management. This report provides an overall summary of Internal Audit work delivered in 2015/16 as well as including the formal annual opinion of the Head of Internal Audit.

Executive Summary

Over the last few years, the Human Fertilisation and Embryology Authority has developed its regulatory model and its status within the NHS and beyond. To achieve its objectives, both executive and non-executive management have undertaken significant work to ensure that the organisation's governance structures including internal control and risk management arrangements are fit for purpose. Internal Audit has continuously provided assurance and advice where appropriate to support management's efforts.

Our opinion is based solely on our assessment of whether the controls in place support the achievement of management's objectives as set out in our 2015/16 Internal Audit Plan and Individual Assignment Reports.

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

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

2015/16 Performance Summary

2015/16 Agreed programme	**3**
Total reviews deferred to complete in 2016/17	**0**
Total reviews added to programme in 2015/16	**1**
Total to deliver 2015/16	**4**
Total reviews completed in 2015/16	**3**
Review to support the data migration within the Register of Treatments project abandoned, as this work is now to be undertaken by a third party	**1**
% of programme completed	**75%**

Total Number of Audits completed by rating (excludes follow up of recs)

Total no reviews completed 2015/16	Substantial	Moderate	Limited	Unsatisfactory	Advisory	Total Rated Work	Advisory Work
3	0	2	0	0	1	**2**	**1**
						66%	**34%**

Resources 2015/16

Period	Full year Budget (man days)	Year to Date			Full year Forecast (man days)
		Budget	Actual	Variance	
April 2015 to March 2016	**42.9**	**42.9**	**41**	**1.9**	**41**

In 2015/16 our programme included two elements of advisory work. One of these involved assurance mapping of capacity and resilience arrangements within HFEA. This work was not rated but the findings are taken into account where relevant in forming our overall opinion for the year. The other element of advisory work was providing support to management in relation to the data migration for the Register of Treatments. This work has now been concluded as management has engaged a third party in this process and so further support from internal audit is not required.

Internal Audit Plan Delivery 2015/16 - Assurance and Advisory Work Summary

#	Audit Title	Status	Outcome	Recommendations agreed by priority		
				High	Medium	Low
1	Requests for Information	Complete	Moderate	0	2	2
2	Incident handling	Complete	Moderate	0	0	6
3	Capacity and Resilience	Complete	No rating – assurance mapping exercise	N/A – No ratings provided		
4	Data Migration - Register of Treatments	Abandoned	No rating – advisory support to management	N/A – No ratings provided		
			Total	**0**	**2**	**8**

Compliance with Public Sector Internal Audit Standards and Quality Assurance

Health Group Internal Audit Services (HGIAS) was subject to an external quality assessment of its services in March 2016, a requirement of HM Treasury which should be undertaken at least every 5 years. Touchstone Renard Limited were commissioned to perform the EQA which is based on a quality assessment framework (The IAQAF). The IAQAF has been designed to help evidence effective internal auditing in line with the Public Sector Internal Audit Standards (PSIAS), with a focus on outcomes that help meet public service delivery commitments. The conclusion can be one of three assessment opinions – Fully Conforms (FC), Generally Conforms (GC) and Partially Conforms (PC) to the above standards. HM Treasury standard requirements are "Generally Conforms".

I am very pleased to advise that, in line with our own internal annual assessments, HGIAS has been rated as Generally Conforms. This is a good result, especially so because of the complex internal audit shared service HGIAS provides.

The report details that in 7 of the 17 IAQAF subsections HGIAS Fully Conforms and in the other 10 sections, Generally Conforms. The following is a high level summary of the report findings:

- **Purpose and positioning** – HGIAS has the appropriate status, clarity of role and independence to fulfil its professional remit.
- **Structure and resources** – HGIAS has the appropriate structure and resources to deliver the expected service.
- **Audit execution** – HGIAS has the processes to deliver an effective and efficient internal audit service.
- **Impact** – HGIAS has had a positive impact on the governance, risk and control environment within the organisation.

The report highlights a number of improvements which can be made to strengthen the service and an action plan has been agreed to address the recommendations made, a number of these have already been actioned. We will ensure that the action plan and progress made is formally reported to the Audit and Governance Committee in due course.

We are particularly pleased that the external assessment acknowledged the complex shared service provided across the health group and the efforts made by all members of the HGIAS team to provide a quality and meaningful service which our customers have acknowledged in their feedback.

Head of Internal Audit Opinion 2015/16

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

My opinion is based on the outcomes of the work that Internal Audit has conducted throughout the course of the reporting year and on the follow up action from audits conducted in the previous reporting year. There have been no undue limitations on the scope of Internal Audit work and the appropriate level of resource has been in place to enable the function to satisfactorily complete the work planned. Internal Audit is fully independent and remains free from interference in determining the scope of internal auditing, performing work and communicating results.

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

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

Therefore, in summary, my overall opinion is that I can give **MODERATE assurance** to the Accounting Officer that the Human Fertilisation and Embryology Authority has had adequate and effective systems of control, governance and risk management in place for the reporting year 2015/16.

Karen Finlayson

Head of Internal Audit

ANNUAL INTERNAL AUDIT PLAN FOR 2016/17

Human Fertilisation and Embryology Authority

Health Group Internal Audit Service

Introduction

This document sets out the internal audit risk assessment and plan for the Human Fertilisation and Embryology Authority (HFEA) for 2016/17.

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

HFEA has identified its overall strategic goals as follows:

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

(These themes are further developed in the HFEA Business Plan, published in March 2016.

The internal audit work that we are planned to undertake during 2016/17 will be focused on governance, internal control, risk management, as well as key strategic and tactical risks faced by the HFEA. Where there are gaps in assurance, audit work will also cover critical activities and their commensurate risks. For this reason, the plan will be subject to review and change, as required during the year, as part of ongoing consultation with management and the Audit and Governance Committee as to the key risk areas.

Internal Audit Policy, Purpose and Responsibilities

Our professional responsibilities as Internal Auditors are set out in the UK Public Sector Internal Audit Standards (UK PSIAS). In line with these requirements, we perform our Internal Audit work with a view to reviewing and evaluating the risk management, control and governance arrangements that the HFEA has in place to:

- Establish and monitor the achievement of the HFEA's objectives.
- Identify, assess and manage the risks to achieving the HFEA's objectives.
- Ensure the economical, effective and efficient use of resources.
- Ensure compliance with established policies, procedures, laws and regulations, including the HFEA's own governance arrangements.
- Safeguard the HFEA's assets and interests from losses of all kinds, including those arising from fraud, irregularity or corruption.
- Ensure the integrity and reliability of information, accounts and data.

Internal Audit Planning 2016/2017

To ensure that internal audit resources are used efficiently, we plan on a risk basis. Therefore, the HFEA's Internal Audit plan is aligned (as closely as possible) to the key strategic risks facing the organisation. Internal audit reviews were selected using the actions below:

- Review of the HFEA's Risk Register to identify key risks, their assurance sources and mitigating actions with a view to providing added assurance where required.
- Consulting with the senior management team.
- Our knowledge of other emerging sector issues.
- Drawing on outcomes from recent internal audit work that remains relevant.

The budget for Internal Audit provision for 2016/17 equates to approximately 40 days of audit work. This document takes into account the budget allocation and has been prepared in consultation with senior management. Internal Audit considers that the programme is sufficient to ensure that HFEA meets its obligations in respect of internal audit.

Risk assessment

Below we consider the current strategic risks facing HFEA before setting out our Internal Audit Plan for 2016/17.

The table below summarises the current high risks according to the HFEA Strategic Risk Register for March 2016, which takes into account its 2016/17 strategic objectives:

Risk area	Description of risk / strategic objective	Residual Risk	April 2016
(1) Legal challenge: Resource diversion	There is a risk that the HFEA is legally challenged in such a way that resources are diverted from strategic delivery. **(Efficiency, economy and value)**	**15 – High**	• Complex and controversial area. • Lack of clarity in HFE Act and regulations, leading to the possibility of there being differing legal opinions from different legal advisers, that then have to be decided by a court. (e.g. one current case challenging the long-held policy position on storage regulations may need to be decided by a court). • Decisions and actions of the HFEA and its committees may be contested. • Subjectivity of judgements means the 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. • HFEA could face unexpected high legal costs or damages which it could not fund. • Legal proceedings can be lengthy and resource draining. • Adverse judgements requiring us to alter or intensify our processes, sometimes more than once.
(2) Information for Quality: 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.	**12 – High**	• Inability to extract reliable data from the Register. • Unable to work out how best to improve CaFC, and/or failure to find out what data/information patients really need. • Stakeholders not on board with the changes. • Cost of delivering better Information becomes too prohibitive, either because the work needed is larger than anticipated, or as a result of the protracted approval periods associated with required DH/GDS gateway reviews.

Risk area	Description of risk / strategic objective	Residual Risk	April 2016
	(Increasing and informing choice – information)		• Redeveloped website does not meet the needs and expectations of our various user types. • Government and DH permissions structures are complex, lengthy, multi-stranded, and sometimes change mid-process. • Resource conflicts between delivery of website and business as usual (BAU). • 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. • New CMS (content management software) is ineffective or unreliable. • Communications infrastructure incapable of supporting the planned changes. • Benefits not maximised and internalised into ways of working. • Potential risks associated with the HFEA's office move in April 2016, in that this will coincide with the delivery period for some IfQ milestones.
(3) Information for Quality: 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)**	**12 – High**	• Poor user acceptance of changes, or expectations not managed. • Clinics not consulted/involved enough. • Scoping and specification are insufficient for realistic resourcing and on-time delivery of changes. • Efficiencies cannot, in the end, be delivered. • Cost of improvements becomes too prohibitive. • Required GDS gateway approvals are delayed or approval is not given. • Benefits not maximised and internalised into ways of working. • Potential risks associated with the HFEA's likely office move in April 2016, in that this will coincide with the delivery period for some IfQ milestones.
(4) Data: Incorrect data released	There is a risk that incorrect data is released in response to a Parliamentary question (PQ), or a Freedom of	**12 – High**	• Poor record keeping. • Excessive demand on systems and overreliance on a few key expert individuals – request overload – leading to errors.

Risk area	Description of risk / strategic objective	Residual Risk	April 2016
	Information (FOI) or data protection request. **(Efficiency, economy and value)**		• Answers in Hansard may not always reflect advice from HFEA. • 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. • Servicing data requests for researchers - poor quality of consents obtained by clinics for disclosure of data to researchers.

Risk assessment mapping

The following table details, by directorate, our risk assessment, the internal audit work completed in 2014/15 and 2015/16, and the internal audit work that it is planned we complete during 2016/17. The total level of coverage to be provided is considered sufficient to ensure Internal Audit undertakes a satisfactory level of assurance work.

Directorate	Key activities	Strategic risks	IA work 2014/15	IA work 2015/16	IA plan 2016/17
Compliance & Information Directorate	• Inspection and Clinical Governance • Business Support - Information and the Register • Development and Analysis	(1) Legal challenge: Resource diversion (2) Information for Quality: Improved information access (3) Information for Quality: Delivery of promised efficiencies (4) Data: Incorrect data released	• Information for Quality (IfQ) • Register of Treatments	• Requests for Information • Data Migration - Register of Treatments	• Cyber penetration testing • Information standards
Strategy & Corporate Affairs Directorate	• Governance and Licensing • Regulatory Policy • Engagement and Communications • Business Planning and Programme Management	(1) Legal challenge: Resource diversion (4) Data: Incorrect data released	• Internal Policies	• Incident Handling • Capacity & Resilience	• Board effectiveness • Assurance mapping
Finance & Resources Directorate	• Budgeting • Accounting • Financial Control • Audit and Risk Assurance • Facilities		• Standing Financial Instructions		• Quality and efficiency of revenue data • Income generation process

Audit reviews included in the 2016/17 plan

Based on review of the strategic risks as above and discussions with HFEA senior management, the table below sets out the proposed reviews within the draft 2016/17 internal audit plan. The table summarises the internal audit plan 2016/17 including indicative timing and estimated audit day allocation, which are both subject to agreement following detailed planning.

Suggested review	Rationale for inclusion	Proposed Scope	Indicative timing and audit day allocation
Income generation process	HFEA receives the majority of its funding from the regulated clinics in form of fee income generated from individual IVF treatments. Those fees, together with licence fees, cover the cost of regulation. Remaining funding is received in the form of grant-in-aid from the sponsors and Department of Health.	This review will evaluate the process and controls within the end to end income generation process, considering how data is used to generate billing.	Q1; 5 days
Quality and efficiency of revenue data		This subsequent review will consider the control of data quality relevant to the billing process and its overall efficiency.	Q2; 4 days
Information standards	Two strategic high risks were identified for information sharing and access to data (3) and (5).	In June/July 2016 HFEA is launching a policy concerning the publication of information on the HFEA's website. This review will consider the information governance arrangements supporting application of the new policy and evaluate the controls in place to ensure published information is up to date and accurate.	Q3; 5 days
Board effectiveness	The evaluation of Board performance is central to good corporate governance. The main goal of Board evaluation is to enable the Board to identify and address any barriers that	This review will assess the Board effectiveness via surveys and interviews, and review of Board papers. We may also agree to observe a board meeting to inform our conclusions.	Q2; 6 days

Suggested review	Rationale for inclusion	Proposed Scope	Indicative timing and audit day allocation
	may impede its effectiveness. Governance contributes to management of all risks and to achievement of corporate objectives.		
Management of Cyber Penetration threat	Cyber threats are of increasing concern to government, public sector and private sector organisations. There are reputational risks should HFEA's network and data be accessed or interrupted, particularly if access was gained to sensitive data.	We will review the cyber security controls put in place by management in relation to HFEA's network, IT and data and the penetration testing performed, and assess whether the arrangements appear to reflect good practice in mitigating the risks which HFEA faces in this area.	Q2, 5 days
Assurance mapping	Following the assurance mapping of capacity and resilience in 2015/16, HFEA management has requested further assurance mapping be included as part of the 2016/17 audit plan.	We will deliver an assurance 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.	Q3; 3 days
Audit management		All aspects of audit management to include: • Drafting the Audit Plan; • Attendance at liaison meetings and HFEA Audit and Governance Committee meetings; • Drafting committee papers/progress reports;	Ongoing; 7 days

Suggested review	Rationale for inclusion	Proposed Scope	Indicative timing and audit day allocation
		• Follow-up work on prior recommendations; • Resourcing and risk management activities; and • Contingency.	
Contingency			5 days
		Total	**40 days**

Action Required

The Audit and Governance Committee is invited to consider:

- whether it agrees with our proposed priorities for reviews;
- the scheduling of proposed reviews over the year; and
- suggest any other key areas for inclusion on the audit plan.

Audit and Governance Committee Paper

Paper Title:	**Information Assurance**
Paper Number:	[AGC (15/06/2016) 500]
Meeting Date:	15 June 2016
Agenda Item:	**9**
Author:	Sue Gallone
For information or decision?	Information
Resource Implications:	None
Implementation	N/A
Communication	N/A
Organisational Risk	Not to have an assessment would undermine the I Governance Statement and improvement required may not be identified and acted upon.
Recommendation to the Committee:	The Committee is asked to note the SIRO's assessment of information governance and discuss.
Evaluation	Annually, to inform the consideration of the annual report and accounts
Annexes	

Information Assurance

Background

1. It is a Cabinet Office (CO) requirement that boards receive assurance about information risk management. This provides for good governance in its own right, ensures that the board is involved in information assurance and informs the Audit and Governance Committee's consideration of the Governance Statement. The Senior Information Risk Officer (SIRO) makes an annual report to the Accounting Officer to inform the Governance Statement and this paper provides that report for the Committee's purposes too. The report is also reviewed by the Senior Management Team (SMT).

2. The Department of Health (DH) usually requires arms length bodies (ALBs) to make a similar report to them, to inform their departmental reporting to CO.

3. My assessment is based on the requirements of the Security Policy Framework (SPF) Security policy framework - Publications - GOV.UK. and the 10 Steps to Cyber Security, the guidance issued as part of the Government's cyber security strategy. We are not reporting using the Information Governance Toolkit, which organisations who deal with patient data are required to use. The HFEA's patient data is not of the same nature or subject to the same processes as in the NHS institutions who report using the more detailed Information Governance Toolkit.

Recommendation

4. Members are asked to note the assessment set out in this paper.

Report

5. The HFEA has a sound culture of protecting information and staff have a good understanding of the need and protocols. There have been no incidents of data loss in 2015/16 and there is a good track record of properly protecting information and systems. Satisfactory penetration testing last took place in March 2012 and the Head of IT performs monthly vulnerability assessments. Further external penetration testing is planned for 2016/17 after the next server upgrade. Policies were updated in 2015/16 and need to be communicated further to staff.

6. The high level assessment of the 10 areas relating to cyber security is:

i. Information risk management – action required to formally risk assess information assets

ii. Secure configuration – considered satisfactory, based on assurances from IT team

iii. Network security - considered satisfactory, based on assurances from IT team

iv. Managing user privileges – satisfactory

v. User education and awareness – policies need to be communicated and assurance sought that these are understood

vi. Incident management – satisfactory

vii. Malware prevention – considered satisfactory, based on assurances from IT team

viii. Monitoring – considered satisfactory, based on assurances from IT team

ix. Removable media controls - satisfactory

x. Home and mobile working – satisfactory.

Assessment of HFEA compliance with the Security Policy Framework 2014
As at May 2016

	Mandatory Requirement	Compliance	Further actions required
1	Departments and Agencies must establish an appropriate security organisation (suitably staffed and trained) with clear lines of responsibility and accountability at all levels of the organisation. This must include a Board-level lead with authority to influence investment decisions and agree the organisation's overall approach to security.	Director of Finance and Resources is SIRO, Head of Information Technology has day to day responsibility. Both are appropriately trained and experienced.	Better communication of any issues to SIRO
2	Departments and Agencies must: * Adopt a holistic risk management approach covering all areas of protective security across their organisation. * Develop their own security policies, tailoring the standards and guidelines set out in this framework to the particular business needs, threat profile and risk appetite of their organisation and its delivery partners.	Risks identified escalated to operational and strategic risk registers as necessary. Policies in place.	Keep policies up to date
3	Departments and Agencies must ensure that all staff are aware of Departmental security policies and understand their personal responsibilities for safeguarding assets and the potential consequences of breaching security rules.	All staff informed of policies and given guidance. Annual training undertaken by all through Civil Srvice Learning.	Further awareness raising with staff
4	Departments and Agencies must have robust and well tested policies, procedures and management arrangements in place to respond to, investigate and recover from security	Head of IT monitors system in place for detecting and responding to security	None

	incidents or other disruptions to core business.	breaches. Business continuity plan in place.	
5	Departments and Agencies must have an effective system of assurance in place to satisfy their Accounting Officer / Head of Department and Management Board that the organisation's security arrangements are fit for purpose, that information risks are appropriately managed, and that any significant control weaknesses are explicitly acknowledged and regularly reviewed.	Head of IT reviews and reports	IT security audit and testing planned
6	Departments and Agencies must have an information security policy setting out how they and any delivery partners and suppliers will protect any information assets they hold, store or process (including electronic and paper formats and online services) to prevent unauthorised access, disclosure or loss. The policies and procedures must be regularly reviewed to ensure currency.	Policies and procedures in place	Further awareness raising and actions to embed
7	Departments and Agencies must ensure that information assets are valued, handled, shared and protected in line with the standards and procedures set out in the Government Security Classifications Policy (including any special handling arrangements) and the associated technical guidance supporting this framework.	The HFEA's assets are all classified OFFICIAL and are appropriately controlled.	None
8	All ICT systems that handle, store and process HMG classified information or business critical data, or that are interconnected to cross-government networks or services (e.g. the Public Services Network, PSN), must undergo a formal risk assessment to identify and	IFQ programme engaged with CLAS consultant. IT security audit of Spring Gardens planned	IT security audit and testing planned

	understand relevant technical risks; and must undergo a proportionate accreditation process to ensure that the risks to the confidentiality, integrity and availability of the data, system and/or service are properly managed.		
9	Departments and Agencies must put in place an appropriate range of technical controls for all ICT systems, proportionate to the value, importance and sensitivity of the information held and the requirements of any interconnected systems.	Access to HFEA data by users strongly controlled by role-specific permissions.	CLAS assessment of IFQ technology.
10	Departments and Agencies must implement appropriate procedural controls for all ICT (or paper-based) systems or services to prevent unauthorised access and modification, or misuse by authorised users.	Policies and staff induction in place.	Records management improvements required
11	Departments and Agencies must ensure that the security arrangements among their wider family of delivery partners and third party suppliers are appropriate to the information concerned and the level of risk to the parent organisation. This must include appropriate governance and management arrangements to manage risk, monitor compliance and respond effectively to any incidents. Any site where third party suppliers manage assets at SECRET or above must be accredited to List X standards.	Delivery partners have provided assurance with regards to information governance and security arrangements	
12	Departments and Agencies must have clear policies and processes for reporting, managing and resolving Information Security Breaches and ICT security incidents.	Policy in place	Promote to staff

13	Departments must ensure that personnel security risks are effectively managed by applying rigorous recruitment controls, and a proportionate and robust personnel security regime that determines what other checks (e.g. national security vetting) and ongoing personnel security controls should be applied.	Recruitment and references provide assurance. No vetting in place.	None
14	Departments and Agencies must have in place an appropriate level of ongoing personnel security management, including formal reviews of national security vetting clearances, and arrangements for vetted staff to report changes in circumstances that might be relevant to their suitability to hold a security clearance.	N/a	
15	Departments must make provision for an internal appeals process for existing employees wishing to challenge National Security Vetting decisions and inform Cabinet Office Government Security Secretariat should an individual initiate a legal challenge against a National Security Vetting decision.	N/a	
16	Departments and Agencies must undertake regular security risk assessments for all sites in their estate and put in place appropriate physical security controls to prevent, detect and respond to security incidents.	Assessment and sufficient controls provided by NICE.	None
17	Departments and Agencies must implement appropriate internal security controls to ensure that critical, sensitive or classified assets are protected against both surreptitious and forced attack, and are only available to those with a genuine “need to know". Physical security measures must be proportionate to level of threat, integrated with other protective	Visitor and entry controls provided by NICE. Lockable furniture provided for storage. Clear desk and clear screen practice in place.	None

	security controls, and applied on the basis of the “defence in depth" principle.		
18	Departments and Agencies must put in place appropriate physical security controls to prevent unauthorised access to their estate, reduce the vulnerability of establishments to terrorism or other physical attacks, and facilitate a quick and effective response to security incidents. Selected controls must be proportionate to the level of threat, appropriate to the needs of the business and based on the “defence in depth" principle.	Sufficient controls in place through NICE	None
19	Departments and Agencies must ensure that all establishments in their estate put in place effective and well tested arrangements to respond to physical security incidents, including appropriate contingency plans and the ability to immediately implement additional security controls following a rise in the Government Response Level.	NICE provide the lead on incidents. HFEA have contingency plans in place that are reviewed annually.	None
20	Departments and Agencies must be resilient in the face of physical security incidents, including terrorist attacks, applying identified security measures, and implementing incident management contingency arrangements and plans with immediate effect following a change to the Government Response Level.	NICE provide the lead on incidents. HFEA have contingency plans in place.	None