Audit and Governance Committee Paper

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

Numerically:

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

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

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

ANNUAL ASSURANCE REPORT 2016/17

Human Fertilisation and Embryology Authority

DRAFT

Health Group Internal Audit Service

Background

In order to be able to provide an annual opinion for 2016/17 to the Human Fertilisation and Embryology Authority's (HFEA) Accounting Officer, it is necessary to consider the work undertaken by Internal Audit over the course of the year, the outcomes of that work and feedback from management on improvements to their areas of responsibility as a result of that work. This together with wider intelligence gathered from all sources of assurance (including the NAO) and performance reporting, inform the Head of Internal Audit's view of controls, governance and risk management.

This report provides an overall summary of Internal Audit work delivered in 2016/17 as well as including the formal annual opinion of the Head of Internal Audit.

Executive Summary

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

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

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

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

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

2016/17 Performance Summary

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

Total Number of Audits completed by rating

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

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

Resources 2016/17

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

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

The reviews completed during the year are summarised below:

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

Compliance with Public Sector Internal Audit Standards and Quality Assurance

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

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

Head of Internal Audit Opinion 2016/17

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

My opinion is based on the outcomes of the work that Internal Audit has conducted throughout the course of the reporting year and on the follow up action from audits conducted in the previous reporting year. Due to budget constraints the programme in any year only covers a small number of areas, but over a three year period we aim to cover a broad range of governance, risk and internal control areas.

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

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

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

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

There have been no undue limitations on the scope of Internal Audit work and the appropriate level of resource has been in place to enable the function to satisfactorily complete the work planned. Internal Audit is fully independent and remains free from interference in determining the scope of internal auditing, performing work and communicating results.

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

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

- In the case of **risk management** Moderate

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

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

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

DRAFT

Karen Finlayson

Head of Internal Audit

NEED TO
INSERT THE HFEA LOGO

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

Government
Internal Audit
Agency

CONTENTS

Section

Page

1. INTRODUCTION

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

2. HFEA CONTEXT

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

HFEA has identified its overall strategic goals as follows:

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

3. INTERNAL AUDIT POLICY, PURPOSE AND RESPONSIBILITIES

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

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

4. INTERNAL AUDIT PLANNING 2017/18

The planning process

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

Audits were therefore selected using the approach outlined below:

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

Planning outcomes

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

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

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

The Audit and Governance Committee are invited to approve:

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

5. PROPOSED AUDIT COVERAGE & AUDIT PLAN 2017/18

5.1 Summary of Audit Coverage

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

Table A: Summary of Audit Topics

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

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

Table B: Resource allocation

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

SUMMARY OF AUDIT RECOMMENDATIONS

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

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

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

4. **Lack of written evidence of approval from the Head of Engagement and/or a Director for six of the eight publications selected for testing.**			
The guidance document requires that corporate publications are subject to appropriate review before release. This includes a final sign off from a Director and/or by the Head of Engagement. During our review we were unable to locate evidence of formal written approval for six publications. In discussion with the Head of Engagement it was stated that verbal approval was provided on each of these occasions and, therefore, this is considered a documentation issue. The publications for which we were unable to review evidence of approval were: 1) Our committees and panels 2) Our partners 3) Making a complaint about a fertility clinic 4) Meet our Authority members/our board 5) Applying to use our data for research 6) Home Page *As the public has access to the new website there is a risk that inaccurate information could be published which could undermine HFEA's stated objective of building trust in their regulation if appropriate review has not been undertaken. In addition, if the publications were of poor quality this might lead to confusion amongst users which may lead to higher levels of individual requests for help and/or guidance, impacting use of resources. If approval is not evidenced, there is greater risk that a publication may be released which has not been appropriately reviewed and approved, which increases these risks.*	All approvals should be in writing to evidence that all publications have been appropriately reviewed and approved, and have a complete audit trail.	We acknowledge this and agree with the recommendation. ***We will clarify the guidance and ensure an email is sent to the author to confirm approval*** **May 2017 update** The guidance says that the approver must always send an email to the author approving the information. This must be recorded in TRIM and referred to in the information production spreadsheet. **Recommendation complete**	***Head of Engagement*** 1 April 2017 8 May 2017 **COMPLETE**
CLOUD CYBER RISK ASSESSMENT (ADVISORY)			
5. **Business Continuity (Advisory)**			
Using a public cloud service such as Microsoft's Azure Cloud requires a network connection to the outside world (internet). A network related incident at the HFEA office could result in staff being unable to access key services hosted on the Azure Cloud	We recommend HFEA to update their Business Continuity policies to ensure it has appropriate plans and procedures in the event of an incident, such as network failure impacting services hosted on the Azure Cloud. This could be something simple as allowing staff to work from a secure environment such as their home via a secure VPN connection.	Agreed. IT staff can already access Azure services from remote locations. General HFEA staff can access Office 365 from home. ***Remote access in place.*** We will investigate divergent route network connectivity for Spring Gardens. ***Divergent route to be investigated*** **May 2017 update** The HFEA has a second wireless connection that can be used in the event of primary internet connectivity failure. **Recommendation complete**	***Head of IT*** ***Complete*** ***by end of April 2017*** **COMPLETE**