AUDIT SCOTLAND BOARD ON 3 MAY 2016 AT THE CONCLUSION OF THE AUDIT COMMITTEE MEETINGS AND HELD IN THE OFFICES OF AUDIT SCOTLAND, 102 WEST PORT, EDINBURGH

A G E N D A

1.	Apologies
2.	Declarations of interest
3.	Chair's Report – Verbal update
4.	Accountable Officer's Report – Verbal update
5.	Accounts Commission Chair's Report – Verbal update
6.	Minutes of the meeting dated 24 March 2016
7.	Minutes of the Audit Committee meeting dated 26 February 2016
8.	Minutes of the Remuneration and Human Resources Committee meeting dated 26 February 2016
9.	Review of the Actions Tracker
10.	2015/16 Annual Report on Freedom of Information and Environmental Information – Report by the Corporate Governance Manager
11.	2015/16 Annual Report on Complaints Handling – Report by the Corporate Governance Manager
12.	Securing World Class Audit: Review of Funding and Fees – Progress and Issues Arising – Report by the Assistant Auditor General
13.	Corporate Plan Update 2016/17 - Report by Assistant Director, Corporate Performance and Risk
14.	Review of Risk Management Framework - Report by Assistant Director, Corporate Performance and Risk
15.	Draft Information Security Management Policy – Report by Assistant Director, Corporate Performance and Risk
16.	Publication of Board Papers – Report by the Assistant Director, Corporate Performance and Risk
17.	AOB
18.	Date of next meeting • **2 June 2016** at the conclusion of the meeting of the Remuneration and Human Resources Committee in the offices of Audit Scotland, 102 West Port, Edinburgh. ***Please submit your apologies to Joy Webber***

Item: 6
Board: 06/2016

Minutes of Meeting of **Audit Scotland** held on 3 May 2016 in the offices of Audit Scotland at 102 West Port, Edinburgh

PRESENT:	I Leitch (Chair) C Gardner H Logan D Sinclair R Griggs
APOLOGIES:	None
IN ATTENDANCE:	D McGiffen, Chief Operating Officer R Frith, Assistant Auditor General M Walker, Assistant Director, Corporate Performance and Risk A Devlin, Corporate Governance Manager

Item No	Subject
1.	Apologies
2.	Declarations of Interest
3.	Chair's Report
4.	Accountable Officer's Report
5.	Accounts Commission Chair's Report
6.	Minutes of the meeting dated 24 March 2016
7.	Minutes of the Audit Committee meeting dated 26 February 2016
8.	Minutes of the Remuneration and Human Resources Committee meeting dated 26 February 2016
9.	Review of the Actions Tracker
10.	2015/16 Annual Report on Freedom of Information and Environmental Information
11.	2015/16 Annual Report on Complaints Handling
12.	Securing World Class Audit: Funding and Fees – Draft Consultation
13.	Corporate Plan Update 2016/17
14.	Review of Risk Management Framework
15.	Draft Information Security Management Policy
16.	Publication of Board Papers
17.	AOB
18.	Date of next meeting

1. Apologies

There were no apologies.

2. Declarations of Interest

Ian Leitch declared his membership of the Scottish Legal Complaints Commission. Heather Logan declared her membership of the Audit and Advisory Committee of the Scottish Public Services Ombudsman (SPSO).

3. Chair's Report

Ian Leitch advised that, since the previous meeting of the Board, he had held regular meetings with Caroline Gardner, Auditor General for Scotland and Diane McGiffen, Chief Operating Officer, to discuss Board matters and had met with Russell Frith, Assistant Auditor General, to discuss the progress of work on fees and funding.

The Chair advised that planning was underway for the Board development event. Following a brief discussion about dates it was agreed that the Chief Operating Officer would liaise with Board members to secure a date in August. The Chair suggested that discussion of the SCPA legacy paper, which had been circulated, should be scheduled for that event.

The Chair further advised that, following discussions with Caroline Gardner, Auditor General and Douglas Sinclair, Chair of the Accounts Commission about the quorum requirements in the Board's Standing Orders, he proposed that the Standing Orders would remain in the meantime, as currently drafted. However, while recognising the rationale for the existing quorum arrangements, the Chair pointed out that, in the event of the absence by either the Auditor General or the Chair of the Accounts Commission, the Audit Scotland Board could not competently meet and no business could be undertaken. Therefore, the Chair requested that there be further discussion on possible options to handle such circumstances at the development event.

Action:

- **The date for the Board development event to be finalised and the Chief Operating Officer would schedule the SCPA legacy paper for discussion together with quorum options at the event. (May – August 2016)**

4. Accountable Officer's Report

Caroline Gardner provided an update on her activity since the previous board meeting, including ongoing development of ways to support the new Parliament, including members' orientation and continuing development.

Caroline advised of the forthcoming publication of a report on 'Common Agricultural Policy Futures programme, An update' on 19 May 2016, in the period between the Holyrood election publication embargo and the European Referendum publication embargo.

Caroline also provided an update on key internal business issues, including the ballot in favour of the pay offer that had been made to the Principal and Civil Service Union at Audit Scotland, who had balloted their members at Audit Scotland on the pay offer for 2016 and had recommended acceptance of the offer. Caroline also advised that a post project review was underway about the West Port office relocation, as was work to secure new accommodation in Inverness and potential work on the Glasgow office. Finally, she

advised that a full programme of internal and external audit work was ongoing to support the presentation of the final accounts to the next Audit Committee and Board meetings.

Douglas Sinclair commented that he had been impressed by the new secondees that he and the Accounts Commission had met at their most recent meeting. Diane McGiffen advised that there had been a recent welcome increase in the number of secondment opportunities and that currently there were four secondees, one each from the Scottish Parliament, UK Statistics Authority, West Lothian Council and Scotland's Rural College.

5. Accounts Commission Chair's Report

Douglas Sinclair provided an update on the work of the Accounts Commission since the previous meeting of the Board. He advised that there had been recent consideration of the best value follow up work on Edinburgh City Council, which had included the transformation plan for the council and its approach to decentralisation.

Douglas advised that the Accounts Commission was paying close attention to discussions about the future shape of local government and health services that were forming part of the election campaign.

6. Minutes of the meeting dated 24 March 2016

The Board considered the note of the meeting of Board members on 24 March 2016, which had been previously circulated. The Board members confirmed the note was an accurate record of the meeting.

7. Minutes of the Audit Committee meeting dated 26 February 2016

The Board considered the note of the meeting of the Audit Committee 26 February 2016, and adopted the minute subject to the minor changes made at the earlier Audit Committee meeting.

8. Minutes of the Remuneration and Human Resources meeting dated 26 February 2016

The Board considered the note of the Remuneration and Human Resources meeting of 26 February 2016, which had been previously circulated. The Board noted that the minutes of the meeting on 24 March 2016 were still to be circulated.

9. Review of the Actions Tracker

The members noted the update provided by the Action Tracker, which had been previously circulated.

Diane McGiffen advised that, in line with the changes agreed for the Audit Committee action tracker, unique identifiers would be added to each item.

10. 2015/16 Annual Report on Freedom of Information and Environmental Information

Alex Devlin, Corporate Governance Manager, joined the meeting.

Alex Devlin, Corporate Governance Manager, introduced the 2015/16 Annual Report on Freedom of Information and Environmental Information report, which had been previously circulated.

Alex invited members to consider the assurance provided on our Freedom of Information (FOI) and Environmental Information Regulations (EIRs) arrangements, requests and performance.

Following discussion, members noted that the assurances provided and that the FOI/EIR arrangements were working well.

11. 2015/16 Annual Report on Complaints Handling

Alex Devlin, Corporate Governance Manager, introduced the 2015/16 Annual Report on Complaints Handling, a copy of which had been previously circulated.

Alex invited members to note the reduction in the number of complaints received and assurance that there are no significant issues to report.

Following discussion, members noted the assurance provided on the handling of complaints during the year and that the process for handling complaints was working well.

Alex Devlin, Corporate Governance Manager, left the meeting.

12. Securing World Class Audit: Funding and Fees – Draft Consultation

Russell Frith, Assistant Auditor General, introduced the report on Funding and Fees – Draft Consultation, a copy of which had been previously circulated.

Russell advised the Board that a lot of work had been completed since the previous Board meeting to develop the underlying models to support greater transparency of fees and had used data from the 2016/17 budget to populate the model. He advised that there was still analysis and discussion required to make a recommendation on where the level of fees should be fixed. He advised that following discussion with Management Team last week, colleagues thought it would be better to complete further analysis on fees and Audit Scotland's efficiency target before providing more detailed information of the content of the planned consultation. He advised that this would result in a delayed but more effective consultation.

The report that the Board was being invited to consider looked at the potential impact of the procurement exercise and identified some of the considerations in setting fees for 2016/17 audits on which early guidance from the Board would be useful. Russell also advised that the final part of the report dealt with the presentation of hourly rates, in response to a previous request from the SCPA.

The Board discussed the contribution that the procurement results make to the overall cost of the public audit model and the contribution that Audit Scotland will make. Diane McGiffen advised that the Management Team would be considering options for the next five years. She outlined the actions that had been taken to reduce the cost of audit by around 25% over the previous five years, including reducing the number of staff employed, by deploying voluntary early release arrangements and recruitment freezes, as well as implementing long term plans to reduce property costs significantly. She also advised that cost reductions had taken place consistently across all business groups.

The Board discussed the decisions which had been taken earlier in the procurement exercise to determine the size and scale of the work to be undertaken by the in-house

team and the firms, and Russell Frith reminded the Board of the range of factors taken into account, including the need for an in-house practice to have a critical mass of work to provide effective competition to the firms, and the views of the Auditor General and the Chair of the Accounts Commission on the additional value offered by the in-house team. The Board also discussed the importance of being able to quantify and cost the added value of the in-house team and of demonstrating value for money and efficiency over the lifetime of the appointments.

The Chair and Heather Logan expressed their concern to understand the implications for the Audit Services Group of the procurement exercise. The Board agreed that the challenge for Audit Scotland was to secure and demonstrate efficiency and reduced costs without sacrificing quality. Caroline Gardner reminded the Board of the importance of the work already undertaken and planned on the costing model which underpins fee setting and of the ability to demonstrate transparency in costing and the apportionment of costs. She advised that, as planned, Russell Frith would bring further reports to the Board on these topics in June, August and September 2016, as set out in the action tracker. It was agreed to consider how the work on Audit Services delivery of best value, which the Board had previously considered, and the added value provided by public audit model could be developed to include costing.

Diane McGiffen advised that the Management Team would be considering the next phase of Audit Scotland's efficiency strategy and the options for setting targets at its next meeting, and that this was central to the preparation of the 2017/18 budget submission.

During discussion, members agreed that it would be helpful to summarise in one place the key decisions taken on the procurement strategy and fees and funding, including the benefits of having an in-house practice.

Caroline suggested, and the Board agreed, that the longer term financial strategy should be modelled over a five year period including fee reductions at various levels above and below 10 per cent alongside the efficiency targets to be set for Audit Scotland's work.

It was agreed that the financial strategy had to balance a number of imperatives including providing assurance to Parliament and the public that audit was providing high levels of assurance and audit quality alongside value for money.

Action(s):

- **Russell Frith to prepare for the next Board meeting:**

  (a) a report on fee setting options, including Audit Scotland's efficiency plans
  (b) a summary of all the decisions taken on procurement
  (c) a draft consultation paper on fees and transparency.
  (June 2016)

- **Russell Frith to prepare proposals for developing the work on demonstrating best value in the delivery of audit and the added value provided by the public audit model to be progressed. (September 2016)**

13. Corporate Plan Update 2016/17

Martin Walker, Assistant Director, Corporate Performance and Risk, introduced the Corporate Plan Update 2016/17 report, which had been previously circulated. Martin invited members to consider and approve the Corporate Plan update for 2016/17.

During discussion, members commended Martin on the clarity of the report and drafting.

Following further discussion, members approved the plan subject to final amendments and a further conversation between Douglas Sinclair and Martin Walker about links with the Accounts Commission strategy.

Action(s):

- **The Assistant Director, Corporate Performance and Risk to arrange for publication of the draft Corporate plan following final discussion and amendment. (May 2016)**

14. Review of Risk Management Framework

Martin Walker, Assistant Director, Corporate Performance and Risk, introduced the report on Review of Risk Management Framework, which had been previously circulated.

Martin invited members to approve the revised risk management framework, subject to any amendments recommended by the Audit Committee.

Members noted the earlier discussion at the Audit Committee and approved the revised risk management framework.

Action(s):

- **The Assistant Director, Corporate Performance and Risk to publish the Review of Risk Management Framework. (May 2016)**

15. Draft Information Security Management Policy

Martin Walker, Assistant Director, Corporate Performance and Risk, introduced the Draft Information Security Management Policy, a copy of which had been previously circulated.

Martin invited members to approve the revised Information Security Management Policy which sets out the overarching principles of information security and the associated roles and responsibilities.

Members noted and approved the updated policy.

Actions:

- **The Assistant Director, Corporate Performance and Risk to publish the Information Security Management Policy. (May 2016)**

16. Publication of Board Papers

Martin Walker, Assistant Director, Corporate Performance and Risk, introduced the report on Publication of Board Papers, which had been previously circulated.

Martin invited members to consider the report together with the guidance on the publication of Board papers to agree the reports to be published on the Audit Scotland website following this meeting.

Members discussed and agreed the reports to be published alongside the approved minute of the meeting.

The reports not for publication were:

- Item 8 Minutes of Remuneration Committee (statutory/security/legal - personal information).
- Item 12 Fees and Funding (effective conduct of business - free and frank provision of advice/exchange of views for the purposes of deliberation/conduct of public affairs).
- Item 13 Corporate Plan (effective conduct of business - information intended for future publication).

Actions:

- **The Assistant Director, Corporate Performance and Risk to arrange to publish the reports on the Audit Scotland website alongside the approved minute. (June 2016)**

17. AOB

There was no further business.

18. Date of Next Meeting

It was noted that the next Audit Scotland Board meeting had been scheduled for **2 June 2016** in the offices of Audit Scotland, 102 West Port, Edinburgh.

Item: 7
Board: 05/2016

Minutes of meeting of the **Audit Committee** of Audit Scotland held in the offices of Audit Scotland, at 102 West Port, Edinburgh on **26 February 2016** at 10:00hrs.

PRESENT: H Logan (Chair)
D Sinclair
R Griggs

APOLOGIES: None

IN ATTENDANCE: I Leitch, Chair of Audit Scotland Board
C Gardner, Auditor General for Scotland/Accountable Officer
D McGiffen, Chief Operating Officer
R Frith, Assistant Auditor General
F McKinlay, Director of Performance Audit and Best Value
M Walker, Assistant Director, Corporate Performance and Risk
C Sweeney, Assistant Director, Performance Audit and Best Value
D Hanlon, Corporate Finance Manager
O Smith, Senior Manager (Procurement and NFI), Audit Strategy
A Devlin, Corporate Governance Manager
C Robertson, BDO LLP Internal Auditors
D Jeffcoat, Alexander Sloan External Auditors

Item No	Subject
1.	Welcome and apologies
2.	Declarations of interest
3.	Minutes
4.	Review of actions tracker
5.	Audit Committee terms of reference
6.	Internal audit progress and reports
7.	Internal audit annual plan 2016/17
8.	Co-operation between internal and external audit
9.	Update on internal audit recommendations
10.	Correspondence handling arrangements
11.	Q3 Financial performance report 2015/16
12.	Timetable for the completion of the statutory accounts to 31 March 2016
13.	Comparison of indicative and agreed fees 2014/15 audits
14.	Review of Risk Register
15.	Risk Interrogation – Failure to maintain efficient access to core systems for ASG
16.	Overview of FRC report on audit systems
17.	External audit plan 2015/16
18.	Business Continuity arrangements annual review
19.	Data incident/loss
20.	Evaluation of Audit Committee effectiveness
21.	AOB
22.	Date of next meeting

1. Welcome and apologies

The Chair advised that a private meeting between the Audit Committee and BDO, internal auditors was held prior to the start of the meeting.

There were no apologies.

The Chair of the Audit Committee informed the members that item 16 on the agenda would be taken after item 10 to aid the sequencing of the agenda. The members agreed to this change.

2. Declarations of Interest

Heather Logan advised that she is a member of the Scottish Public Services Ombudsman Audit and Advisory Committee and that she will demit that role when her current term ends.

3. Minutes

The Audit Committee members reviewed the minutes of the meeting of 3 December 2015, which had been previously circulated.

The minutes were approved as an accurate record.

4. Review of Actions Tracker

The Audit Committee reviewed progress made on outstanding actions and the dates for implementation of the actions.

The Audit Committee members noted progress on outstanding actions.

5. Audit Committee Terms of Reference

The Chair invited comments from members on the paper submitted by the Corporate Governance Manager, which had been previously circulated. The paper advised that there had been a few minor changes to the Terms of Reference.

It was noted that all the planned meetings for 2016 were to be held in Edinburgh and that in doing so limited the accessibility of the Audit Committee and Board members to staff outwith Edinburgh.

After discussion the Chief Operating Officer agreed to revisit the meeting venues for later in the year once the Queen Street station disruption had finished.

The Audit Committee approved the changes and noted the report.

Action(s):

- **The Chief Operating Officer to review meeting venues for later in the year for possible meetings in Glasgow. (June 2016)**

6. Internal Audit Progress and Reports

Fraser McKinlay, Director, Performance Audit and Best Value and Claire Sweeney, Assistant Director, Performance Audit and Best Value, joined the meeting.

Claire Robertson, BDO introduced the internal audit progress report and three internal audit reports, which had been previously circulated.

(a) Internal audit progress report

Claire Robertson informed the members that the 2015/16 programme of internal audits was on track for completion as planned.

The Chair invited comments and questions from the members in relation to the progress report.

The Audit Committee noted the report.

(b) Procurement of audit firms audit report

Claire Robertson informed the members that the audit achieved substantial assurance with only one recommendation. The members were informed that the audit found that Audit Scotland was transparent in its approach to audit procurement and that the procurement strategy was followed.

The Chair invited comments and questions from the members in relation to the report.

Following discussion the Committee noted the report.

(c) Communications and stakeholder engagement audit report

Claire Robertson informed the members that the audit achieved reasonable assurance and that there were two recommendations, one relating to an overarching communications strategy and one on social media.

The Chair invited comments and questions from the members in relation to the report.

Russel Griggs asked if the Audit Committee or Board had oversight of Audit Scotland's strategies. Fraser McKinlay informed the members that he and Management Team had not brought communications and engagement strategies to the Audit Committee/Board, but would consider this. The Chair asked whether the communications strategy was linked to the Corporate Risk register, noting the inter-relationship between the two.

The Chair of the Audit Committee requested that the annual assurance and control map be reissued to members to show the reporting process and timeline for 2016.

The Chair of the Accounts Commission noted that the Auditor General and the Accounts Commission also carried out a wide range of stakeholder engagement, but they had not been interviewed as part of the audit. He also noted that the report did not cover the Commission's engagement plan. Responding to a question from the Chair, he confirmed that retrospective work was not required, but noted that future internal audit work which covered Commission activity may benefit from consultation with the Secretary to the Commission.

The Chair of the Audit Committee asked if the timescales were achievable for implementing the recommendations. Assurance was given that the timescales were achievable and that the recommendations would be taken forward by James Gillies, Communications Manager.

The Committee noted the report.

Action(s):

- **The Chief Operating Officer to reissue the annual assurance and control map to members. (May 2016)**

PABV programme development

Claire Robertson informed the members that the PABV programme development audit highlighted substantial assurance and that the auditors identified areas of good practice in what Audit Scotland was doing. Claire Robertson provided an overview of why each of the four low level recommendations was made.

The Chair invited comments and questions from the members in relation to the report.

The Chair of the Accounts Commission informed the members that he was surprised by the report saying that the programme was subject to approval by the Auditor General and the Accounts Commission but the Secretary to the Commission was not interviewed as part of the audit. The Chair of the Accounts Commission also highlighted that the report did not cover the Commission's statutory requirements around consultation. Claire Robertson suggested that further work could be conducted to address these issues; however the Chair to the Accounts Commission stated that no further work was required. He also suggested that consideration should be given to interviewing the Secretary to the Accounts Commission in future audits where the Commission's arrangements should also be covered.

The Committee noted the report.

Action(s):

- **The Chief Operating Officer to ensure that interests of the Auditor General and the Accounts Commission are considered at the scoping stage of internal audits. (May 2016)**

Claire Sweeney, Assistant Director, PABV left the meeting.

7. Internal Audit Plan 2016/17

Claire Robertson, BDO introduced the draft internal audit plan for 2016/17 which had been previously circulated.

The Chair invited comments and questions from the members in relation to the plan.

The members raised the following points:

- Whether resource management be included in the plan as a result of the comments from SCPA. The Chief Operating Officer suggested that this may be covered in the VfM audit and she would discuss scoping options with Claire.

- Whether there is a process in place for scanning future resource requirements due to changes in the environment e.g. further fiscal devolution and the outcome of the EU referendum. Again, this was suggested that it could be covered under the VfM audit.

- That the references to Audit Scotland's corporate vision should make it clear that these support the principles contained within Public Audit in Scotland and reflect

the new approach to the audit of Best Value. BDO agreed to reword this section of the plan.

Following discussion the Audit Committee approved the 2016/17 internal audit plan.

Action(s):

- **Claire Robertson, BDO to amend and reissue the 2016/17 internal audit plan. (May 2016)**

- **Chief Operating Officer and Claire Robertson, BDO to discuss the scoping of the VFM audit. (May 2016)**

8. Co-operation between internal and external audit

Claire Robertson, BDO introduced the report on co-operation between internal and external audit which had been previously circulated.

David Jeffcoat, Alexander Sloan's informed the members that they were satisfied with the process.

The Audit Committee noted the report.

9. Update on Internal Audit Recommendations

The Corporate Governance Manager submitted an update report on the implementation of Internal Audit Recommendations, which had been previously circulated. The Corporate Governance Manager informed the members that the report now only contained recommendations that have not been previously reported to the Committee as complete, as requested at the Audit Committee meeting in December 2015.

The Chair welcomed the new format of the report and invited comments and questions from the members on the report.

The Chair asked if we were at risk of not meeting the planned dates for the achievement of ISO 27001. The Chair was informed that although ISO work had been re-scheduled to prioritise resources on the Edinburgh office move we were confident in meeting the revised timescales.

Russel Griggs asked if there should be a review of the Audit Committee meetings and reports at the end of the meeting. The Chair informed the member that this would be covered at the end of the meeting under AOB.

Following the discussion the Audit Committee noted the report.

10. Correspondence Handling Arrangements

The Director of Performance Audit and Best Value gave a verbal update on the work undertaken to improve Audit Scotland's performance in handling issues of concern raised through correspondence.

The members were informed that there had been a major review of our processes and that there was now a full time correspondence manager dealing with issues of concern, and that this had contributed to significant improvement in performance.

The Chair invited comments and questions from the members. The members raised the following points:

- What would happen if the issue of concern related to a public body audited by a firm appointed by the Accounts Commission or Auditor General? The members were advised that the issue would be passed to the firm and that Audit Scotland would be kept informed of the outcome.

- Should Audit Scotland communicate better externally on what we can and can't do when issues of concern were raised by members of the public? The Director of Performance Audit and Best Value informed the members that we have made good progress in this area and that we do publish guidance for correspondents and suggested that he provides a paper on correspondence handling for a future meeting.

The Audit Committee welcomed the update.

Action(s):

- **The Director of Performance Audit and Best Value to provide a paper on the correspondence process at a future meeting. (June 2016)**

11. Overview of FRC Report on Audit Systems

The Chair of the Audit Committee brought forward this item.

The Assistant Auditor General introduced an overview report of the FRC on Audit Systems, which had been previously circulated.

The Chair invited comments and questions from the members in relation to the report.

The members asked if there were any significant concerns on the quality of the audits and how any concerns were raised with the Auditor General, the Accounts Commission or the Audit Committee. The members were informed that any quality concerns would be raised with the appointed auditor directly and, where appropriate, would be reported to the Audit Committee.

The Auditor General informed the members that there is a continual check on quality for the Accounts Commission and the Auditor General and that she had asked the Assistant Auditor General to look at quality as part of the procurement process for the next round of auditor appointments.

The Chair asked if Audit Scotland or the AGS/Accounts Commission should be advising Audit Committees to ask their auditors about monitoring reviews and any findings to enhance oversight. The Auditor General agreed that this was a good point for her and the Accounts Commission and they would look at what they might communicate to Audit Committees.

The Audit Committee noted the report.

Fraser McKinlay, Director, Performance Audit and Best Value left the meeting.

12. Q3 Financial Performance Report 2015/16

There was submitted a report by the Corporate Finance Manager on Audit Scotland's Q3 Financial Performance, which had been previously circulated.

The Chair invited comments and questions from the members.

The Chair sought clarification on the fees agreed with bodies for additional work and if the timing of the work and agreement of the fee could affect Audit Scotland's budget. The Chair of the Board informed the members that fees was an item on the Board agenda and that questions on this should be reserved for the Board meeting.

The Chair sought clarification on why consultancy costs were higher than budget. The Chair was advised that additional work was undertaken on the Building a Better Organisation initiative.

The Audit Committee noted the report.

13. Timetable for the completion of the Statutory Accounts to 31 March 2016

There was submitted a report by the Corporate Finance Manager on the Timetable for the completion of the Statutory Accounts to 31 March 2016, which had been previously circulated.

There were no comments or questions from the members on the timetable. The members approved the proposed timetable for the completion of the statutory accounts for the year ended 31 March 2016.

14. Comparison of Indicative and Agreed Fees 2014/15 Audits

Owen Smith, Senior Manager (Procurement and NFI) Audit Strategy joined the meeting.

The Assistant Auditor General and Senior Manager (Procurement and NFI) Audit Strategy, introduced a report on the comparison of indicative and agreed 2014/15 audit fees, which had been previously circulated.

There were no comments and questions from the members in relation to the report.

The Audit Committee noted the report.

Owen Smith, Senior Manager (Procurement and NFI) Audit Strategy left the meeting.

15. Review of Risk Register

There was submitted a report by the Assistant Director, Corporate Performance and Risk, on the review of Audit Scotland's risk register, which had been previously circulated. The members were informed that there was one 'red' risk and that it would be covered under agenda item 15.

The Chair invited comments and questions from the members on the report.

Russel Griggs asked if the register covered the impact of external changes on the organisation's resources and the ability to respond to them. The Assistant Director, Corporate Performance and Risk informed the members that although there was not a specific risk for this, it was covered by a number of the other risks on the register.

The Chair of the Audit Committee challenged the use of internal audit as a control measure in the register. The Chair was informed that Audit Scotland views internal audit as an independent check on mitigating controls. The Chair also asked the Assistant Director, Corporate Performance and Risk to review the content under 'active monitoring' in the next version of the risk register and consider the use of detective controls.

Following the discussion on individual risks and the mitigating actions the members noted the report.

Action(s):

- **The Assistant Director, Corporate Performance and Risk to review the control measures and how best to indicate when a change in the risk assessment would be expected in light of the planned actions. (May 2016)**

16. Risk Interrogation – Failure to maintain efficient access to core systems for ASG

There was submitted a report by the Assistant Director, Corporate Performance and Risk, on the interrogation of risk twelve – failure to maintain efficient access to core systems for ASG, which had been previously circulated.

The Assistant Director, Corporate Performance and Risk provided an update to the members on the current actions to mitigate this 'red' risk and to address reduced performance in the MKI system.

A discussion followed on the cost to Audit Scotland of this reduction in performance and if the reduction could be traced to Audit Scotland's or our suppliers actions. The Chief Operating Officer informed the members that we were investigating this, including looking at the experience of the other UK audit agencies who also use MKI. The members were also informed that we would be seeking external assistance to identify and evaluate options for alternative systems.

The Audit Committee noted the report.

17. External Audit Plan 2015/16

The external auditors, Alexander Sloan submitted the external audit plan for 2015/16, which had been previously circulated.

David Jeffcoat informed the members that the timescale between the end of the audit, the audit clearance meeting and the approval of the accounts was very tight this year and that he would make the draft management letter available to the Audit Committee as quickly as possible prior to the meeting on 2 June 2016.

The Audit Committee noted the report.

18. Business Continuity Arrangements Annual Review

The Corporate Governance Manager submitted a report on Audit Scotland's Business Continuity Arrangements, which had been previously circulated.

The Audit Committee welcomed the comprehensive and clear plans and arrangements.

The members noted the report.

19. Data Incident/Loss

The Corporate Governance Manager had submitted a report on Data Incidents/Loss, which had been previously circulated.

The Corporate Governance Manager highlighted that one of the incidents related to the use of personal email addresses for distributing controlled and personal information and this was contrary to Audit Scotland's Information Security and Data Protection policies. In addition, this constituted a risk to Audit Scotland's reputation and therefore should be discontinued.

The Audit Committee welcomed the report and supported the cessation of using personal email addresses for distributing controlled and personal information in support of our information security policies.

20. Evaluation of Audit Committee Effectiveness

The Assistant Director, Corporate Performance and Risk, submitted a report on the process for evaluating the effectiveness of the Audit Committee over 2015/16, which had been previously circulated.

The Audit Committee agreed to reissue and complete the Audit Committee self-assessment checklist for 2015/16.

Action(s):

- **The Assistant Director, Corporate Performance and Risk to distribute the checklist for completion and report back to the next Audit Committee on findings. (May 2016)**

21. Any Other Business

The Chair of the Audit Committee reminded members that as part of the 2014/15 Audit Committee effectiveness self-assessment that they should review the standard of the papers submitted to them and the effectiveness of their meetings for any improvements.

After discussion the members agreed to arrange a discussion on how this would be best achieved.

Action(s):

- **The Chief Operating Officer to arrange a discussion with the members about reviewing the standard of reports to the committee and the effectiveness of the meetings. (May 2016)**

22. Date of Next Meeting

The next meeting will be held on **3 May 2016** in the offices of Audit Scotland, 102 West Port, Edinburgh. The date and time of the meeting are to be confirmed following clarification of Committee member's availability.

AUDIT SCOTLAND ACTION TRACKER 2016

Item 9

FORUM	Agenda Item No	Item Title	Action Description	Meeting Date	Due Date	Responsible	Assigned to	Complete/Ongoing	Reported Yes/No	Progress Notes
Board	12 (a)	Securing World Class - Ethical Standards	Board members to consider whether any transistional arrangements need to be put in place for existing appointments.	03/12/2015	31/01/2016	All members	All members	Complete	Yes	The Board agreed on 24/03/2016 that this action has been concluded.
Board	7	Review of Actions Tracker	The Action tracker to be revised to include a deadline of May 2016 for the approval of the Corporate Plan.	26/02/2016	03/05/2016	Diane McGiffen	Martin Walker	Complete	No	The report at item 13 of the Board agenda will be considered on 03/05/2016.
Board	10	Q3 Corporate Performance	Russell Frith, Assistant Auditor General, to consider whether performance reports could include more information on audit quality	26/02/2016	03/05/2016	Russell Frith	Russell Frith	Ongoing		
Board	12(b)	Funding and Fees – 2016 Issues and Work Plan	The Assistant Auditor General to prepare a report for Board consideration	26/02/2016	24/03/2016	Russell Frith	Russell Frith	Complete	Yes	The report at item 12(b) of the Board agenda was considered on 24/03/2016.
Board	12(b)	Funding and Fees – 2016 Issues and Work Plan	The Assistant Auditor General to prepare a consultation report for Board consideration	26/02/2016	03/05/2016	Russell Frith	Russell Frith	Complete	No	The report at item 12 of the Board agenda will be considered on 03/05/2016.
Board	12(b)	Funding and Fees – 2016 Issues and Work Plan	The Assistant Auditor General to report on the 2015/16 accounts for Board approval	26/02/2016	02/06/2016	Russell Frith	Russell Frith	Ongoing		This is scheduled for discussion at the Board meeting on 2 June 2016.
Board	12(b)	Funding and Fees – 2016 Issues and Work Plan	The Assistant Auditor General to report on the final proposed fee strategy	26/02/2016	18/08/2016	Russell Frith	Russell Frith	Ongoing		This is scheduled for discussion at the Board meeting on 18 August 2016.
Board	12(b)	Funding and Fees – 2016 Issues and Work Plan	The Assistant Auditor General to report on 2017/18 budget assumptions	26/02/2016	18/08/2016	Russell Frith	Russell Frith	Ongoing		This is scheduled for discussion at the Board meeting on 18 August 2016.
Board	12(b)	Funding and Fees – 2016 Issues and Work Plan	Board approval of 2017/18 budget and 2016/17 audit fees	26/02/2016	15/09/2016	Russell Frith	Russell Frith	Ongoing		This is scheduled for discussion at the Board meeting on 15 September 2016.
Board	13	Openess and Transparency of Board Business	advise the Board of a start date for the new approach to publishing board papers	26/02/2016	24/03/2016	Diane McGiffen	Martin Walker	Complete	Yes	The report at item 13 of the Board agenda will be considered on 24/03/2016.
Board	13	Openess and Transparency of Board Business	The Assistant Director, Corporate Performance and Risk to develop operational guidance to sit alongside the principles presented in the report for the Board to consider	26/02/2016	24/03/2016	Martin Walker	Martin Walker	Complete	Yes	The report at item 11 of the Board agenda was considered on 24/03/2016.
Board	13	Openess and Transparency of Board Business	The quorum for Board meetings to be discussed at the next meeting.	26/02/2016	24/03/2016	Martin Walker	Martin Walker	Complete	Yes	Discussion of the report at item 15 of the Board agenda 24/03/2016 was deferred to the next meeting on 03/05/2016.
Board	11	Audit Scotland Report and Accounts	The Communications Manager will report on Audit Scotland Annual Report and Accounts.	24/03/2016	02/06/2016	James Gillies	James Gillies	Ongoing		This is scheduled for discussion at the Board meeting on 02/06/2016.
Board	12(a)	Funding and Fees - Fee Setting Policies	The Assistant Auditor General to report on the impact of the proposed policies and bring a draft consultation paper to the next meeting of the Board.	24/03/2016	03/05/2016	Russell Frith	Russell Frith	Ongoing		The report at item # of the Board agenda will be considered on 03/05/2016.

Board	12(b)	New Financial Powers Update	The Assistant Director, Audit Services Group will provide an update on the New Financial Powers.	24/03/2016	15/09/2016	Mark Taylor	Mark Taylor	Ongoing		This is scheduled for discussion at the Board meeting on 15 September 2016.
Board	13	Openess and Transparency: Publication of Board Papers	The Assistant Director, Corporate Performance and Risk to issue the operating	24/03/2016	31/03/2016	Martin Walker	Martin Walker	Complete	No	The guidance was issued to staff on 28/03/2016.
Board	13	Openess and Transparency: Publication of Board Papers	The Chief Operating Officer to schedule a future agenda item to review the arrangements.	24/03/2016	01/12/2016	Diane McGiffen	Diane McGiffen	Ongoing		This is scheduled for discussion at the Board meeting on 1 December 2016.
Board	14	Evaluation of Board Effectiveness	The Chief Operating Officer to identify potential dates and develop options for a facilitated session.	24/03/2016	03/05/2016	Diane McGiffen	Diane McGiffen	Ongoing		Progressing and a verbal updddate will be provided at the meeting on 03/05/2016.
Board	14	Evaluation of Board Effectiveness	The Assistant Director, Corporate Performance and Risk to refine the self evaluation questionnaire.	24/03/2016	03/05/2016	Martin Walker	Martin Walker	Complete		Self evaluation document distributed 26/04/16
Board	15	Discussion on Standing Orders	The Chief Operating Officer to schedule a future agenda item to further discuss.	24/03/2016	03/05/2016	Diane McGiffen	Diane McGiffen	Ongoing		This item will be covered as part of item 3, Chair's report on 03/05/2016.
Board	16	AOB	The Chief Operating Officer to circulate a copy of the PAC legacy paper to Board members.	24/03/2016		Diane McGiffen	Diane McGiffen	Complete	No	The Chief Operating Officer circulated the SCPA Legacy paper to members on 15/04/2016.

AUDIT SCOTLAND BOARD

3 MAY 2016

REPORT BY THE CORPORATE GOVERNANCE MANAGER

2015/16 ANNUAL REPORT ON FREEDOM OF INFORMATION AND ENVIRONMENTAL INFORMATION

---

1. Purpose of Report

This is the annual report to the Board on our Freedom of Information (FOI) and Environmental Information Regulations (EIRs) arrangements, requests and performance.

The report concludes that our FOI/EIR arrangements are working well and that there are no significant issues that should be brought to the attention of the Board.

The Board is invited to note the contents of this report.

2. Background

Audit Scotland, the Auditor General and the Accounts Commission are subject to the Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (EIRs).

Audit Scotland developed and implemented suitable joint arrangements for the discharge of FOISA/EIRs in 2005 for all three bodies. These arrangements are reviewed annually.

The Scottish Ministers' Code of Practice on the discharge of functions by Scottish public authorities under FOISA and the EIRs require us to monitor our handling of information requests.

Since 1 April 2013 public bodies are required to submit their FOI and EIR handling statistics, on a quarterly basis, to the Scottish Information Commissioner (SIC). Audit Scotland has complied timeously with this requirement.

3. FOI/EIR Overview for 2015/16

This annual report has been prepared to fulfil our FOI/EIR good practice requirements under the Scottish Ministers section 60 Code of Practice and incorporates our SIC quarterly returns.

Governance

The Knowledge, Information and Technology Governance Group (KITGG) provide oversight of our FOI/EIR arrangements and report their activity to Management Team, the Audit Committee and the Board as necessary. The Corporate Governance Manager is responsible for day-to-day management of our FOI/EIR arrangements.

The FOI/EIR policy was reviewed by the KITGG, re-approved by the Board in August 2015 and staff acknowledge compliance with the policy via the Fit and proper form in November 2015.

Approach to requests

It is our policy to be as open and transparent as possible, and therefore our approach to FOI/EIR requests is to treat them as a 'business as usual' activity. This means that where we would normally supply information to those we work with we will continue to do so without treating them as FOI/EIR requests.

For complex 'business as usual' requests and all other requests, which may have to be considered by an FOI panel, these are recorded in our FOI/EIR system.

Where it is appropriate and legal we can apply exemptions and exceptions to the information being requested. Audit Scotland has established a group of senior managers (FOI panel) trained in applying FOI/EIR exemptions and exceptions to complex requests.

The following statistics and analysis are based on our recorded FOI/EIR requests for 2015/16.

Statistics and Analysis

Number of requests received

Audit Scotland recorded 65 FOI and no EIR requests this year. These were received in:

	2015/16 requests		2014/15 requests	
	FOI	EIR	FOI	EIR
Q1 (April – June)	14	0	14	0
Q2 (July – September)	16	0	29	0
Q3 (October – December)	26	0	14	0
Q4 (January – March)	9	0	16	0
Total	**65**	**0**	**73**	**0**

Sixty were addressed to Audit Scotland, three to the Accounts Commission and two to the Auditor General.

Type of requester

We categorise the requests we receive for analysis purposes. This year we received:

2015/16 requester type	2015/16 requests		2014/15 requests	
	FOI	EIR	FOI	EIR
Commercial organisations	7	0	3	0
Media	10	0	31	0
MSP/MP	3	0	2	0
Organisation	16	0	12	0
Members of the public	25	0	24	0
Public body	2	0	1	0
Other	2	0	0	0

Themes emerging from the requests received

Themes emerging from the information being requested are:

- 32% - AS: staff , finance, cars
- 24% - ICT: equipment, contracts
- 21% - AS: reports, draft & correspondence
- 13% - Data held on other organisations
- 3% - AS: policies, procedures
- 3% - Non IT contracts
- 3% - Other
- 1% - AS Governance

Responding to requests

All information requested was released in full on 46 occasions, partially released on 6 occasions, and the information requested was not held by us on 11 occasions. Two are ongoing.

Cost of administrating and responding to requests

We do not record the actual time spent on specific requests as this is generally covered by the job code for the work information is being requested about. In addition the time spent on FOI/EIR training is coded to the general training and development job code.

However, 10 members of staff recorded 459 hours for administering our FOI systems and procedures, replying to some requests and dealing with complex requests at FOI panels. This equates to approximately £28,000 using the average hourly rate from the Time Recording System. However, the true cost to Audit Scotland of complying with FOI/EIRs will be higher due to the way some FOI/EIR work and training is recorded.

Time taken to respond

FOISA and the EIRs require public bodies to reply to requests within 20 working days and within 40 working days for complex or volumous EIRs. Audit Scotland met this requirement on 60 (94%) occasions and failed to meet it on three (5%) occasions (note two are ongoing). This is a slight deterioration from last year's

98.6% and was the result of extensive consultation with third parties on personal and commercial information prior to release of information.

Charging for dealing with requests

Public bodies are able to make certain charges for dealing with FOI and EIR requests. Where this is appropriate we issue a fee notice. We issued no fee notices in 2015/16.

Public bodies are also able to refuse a request where it will cost more than £600 to deal with it. However, where public bodies estimate the cost to be greater than £600 they are to inform the requester that they may be able to supply some information if they narrow their request. No requests were refused by Audit Scotland on excessive cost of compliance this year.

FOI/EIR panels, reviews and appeals

Panels met ten times this year to consider applying exemptions to some or all of the information being requested. In eight cases we applied exemptions to the information we held. The most commonly used exemptions this year were for 'personal information', 'commercial interests and the economy' and prejudice to effective conduct of public affairs.

Where an applicant is not satisfied with our response to their request they can ask Audit Scotland for a review. We use different FOI/EIR panel members for this task. In 2015/16 there were two requests for a review.

If an applicant remains dissatisfied with how we dealt with their request after a review they can make an appeal to the SIC. There was no appeals to the SIC from dissatisfied applicants this year.

Information requested but not held by Audit Scotland

Audit Scotland issued 11 FOISA section 17 notices this year informing the applicant that the information they were requesting was not held by Audit Scotland, the Auditor General or the Accounts Commission.

Information otherwise accessible

Where the information requested is already publically available eg in the authorities publication scheme/website the public authority does not need to provide it. However, there is a duty to provide advice and assistance, which means informing the requester where the information is published.

Audit Scotland issued two formal section 25 notices informing the applicant that the information was publically available.

FOI/EIR Training

Audit Scotland staff undertake basic FOI/EIR training when they join Audit Scotland. Refresher training is given as necessary. In addition staff updates are published when changes occur. A staff brief was issued in September 2015 and on FOI Day in March 2016 to remind staff of our FOI/EIR arrangements, performance and changes to legislation.

Maintaining training records is dynamic process due to staff joining and leaving the organisation at any point during the year and at the 31 March 2016 only two people had FOI/EIR training outstanding.

4. Recommendation

The Board is invited to note the content of this report.

Item: 11
Board: 05/2016

AUDIT SCOTLAND BOARD

3 MAY 2016

REPORT BY THE CORPORATE GOVERNANCE MANAGER

2015/16 ANNUAL REPORT ON COMPLAINTS HANDLING

---

1. Purpose of Report

This is the annual report to the Board on complaints received by Audit Scotland. This report forms part of a suite of assurance reports in support of the Accountable Officer's governance statement in the annual report and accounts.

The report on complaints handling concludes that there are no significant issues that should be brought to the attention of the Board.

The Board are invited to note the contents of this report.

2. Background

The Public Services Reform (Scotland) Act 2010 (the Act) required the Scottish Public Services Ombudsman to introduce a set of complaint handling principles, which all public bodies have to adhere to.

Audit Scotland, the Auditor General and the Accounts Commission introduced a joint complaints handling process in December 2012. The joint complaints handling process was reviewed and updated in late 2014. A further update to our guides for staff and members of the public was undertaken in November 2015.

A feature of the arrangements is to systematically analyse the complaints received and report on them to Management Team and the Board.

This is the third annual report on complaints handling under our new complaints handling procedure.

3. Complaints received

Audit Scotland staff actively engage with the public through a number of channels for example: the inspection period for local government unaudited accounts, the correspondence process, freedom of information requests, our main office receptions, our telephone switchboard, etc. If our interaction with the public is handled well it enhances our reputation and contributes to our goal of becoming world class. However, if handled poorly it may harm our reputation and lead to dissatisfaction and complaints.

The complaints handling review in late 2014 found that Audit Scotland needed to do more to identify and learn from the complaints it received. Work was

undertaken with the correspondence team to identify complaints from the correspondence process and this resulted in a jump in the number of complaints identified for 2014/15.

The correspondence team continued to refine their corresponding handling processes in 2015/16. As a result of improvements in correspondence handling performance the number of complaints being submitted or identified has fallen.

Complaints are mostly dealt with at stage 1, front line resolution within five working days. Where complaints are more complex or are not resolved at stage 1 they are investigated at stage 2, within 20 working days.

Corporate Services maintains the register of complaints received. The register shows that there were four complaints received in 2015/16 (13 in 2014/15).

Table 1 below shows the number of complaints received and recorded by quarter and the stage they were dealt at. Table 2 details the number of complaints received during the last three years.

Table 1 – Number of complaints received by quarter in 2015/16

	Received	**Stage 1**	**Stage 2**	**In progress**	**Rejected**
Q1	3	1	2	0	0
Q2	1	1	0	0	0
Q3	0	0	0	0	0
Q4	0	0	0	0	0
Total	**4**	**2**	**2**	**0**	**0**

Table 2 – Number of complaints over the last three years

	Received	**Stage 1**	**Stage 2**	**Rejected**
2015/16	4	2	2	0
2014/15	13	8	3	2
2013/14	3	0	2	1

All four complaints resulted from failing to meet published correspondence handling timescales. Although the complaints were received in quarter 1 and 2 of 2015/16 they referred to issues communicated to us in 2014/15. As can be seen from the tables above as the correspondence arrangements and performance have improved the number of complaints emerging has fallen.

This is a good example of when ‘getting it right first time’ reduces the risk to our reputation and helps avoid on-costs with dealing with complaints.

4. Scottish Public Services Ombudsman (SPSO)

The Scottish Public Services Ombudsman Act 2002 (the Act) provides a framework for matters that can be considered by the SPSO for investigation. This year no complaints investigated by Audit Scotland under our complaints handling process were appealed to the SPSO.

However, the SPSO received one complaint about Audit Scotland’s handling of an issue of concern and conclusions in our report – *review of issues around the Lennoxtown Initiative* published on the Audit Scotland website in November 2015. The SPSO’s office reviewed the information submitted by the

complainant and informed the complainant that the matter raised fell outwith their remint under the Act and that no further action would be taken by the SPSO.

5. Conclusions

Our complaints handling process and procedures generally work well. We try to resolve as many complaints at stage 1 with the complainant; however a number will reach the investigation stage. With the improving performance in correspondence handling there has been a corresponding reduction in the number of complaints received this year.

6. Recommendation

The Board is invited to note the contents of this report.

Item: 14
Board: 05/2016

AUDIT SCOTLAND BOARD

3 MAY 2016

REPORT BY THE ASSISTANT DIRECTOR, CORPORATE PERFORMANCE AND RISK

REVIEW OF RISK MANAGEMENT FRAMEWORK

1. Purpose of Report

This report invites the Board to approve the revised risk management framework, subject to any amendments recommended by the Audit Committee.

2. Background

The Board agreed the 'Policy, strategy and assurance framework' at its meeting on 22 January 2015.

The framework was reviewed by the Performance and Risk Management Group during March 2016 and a number of amendments were proposed. The Management Team considered and agreed these at its meeting on 12 April 2016.

The Audit Committee will consider the framework at its meeting on 3 May in advance of the Board meeting.

3. Recommendation

The Board is invited to approve the revised framework subject to any proposed amendments and recommendations from the Audit Committee.

Audit Scotland

Risk management framework

AUDIT SCOTLAND

Prepared for Audit Scotland Board
May 2016

Version control	
Board approval of policy, strategy and framework	January 2015
Review by Performance and Risk Management Group	March 2016
2016 Review by Management Team	April 2016
2016 Review and approval by Audit Scotland Audit Committee and Board	May 2016

Audit Scotland is a statutory body set up in April 2000 under the Public Finance and Accountability (Scotland) Act 2000. We help the Auditor General for Scotland and the Accounts Commission check that organisations spending public money use it properly, efficiently and effectively**.**

Contents

Introduction

1. Audit Scotland provides the Auditor General and the Accounts Commission with the services they need to check that public money is spent properly, efficiently and effectively.

2. The risks we identify in the organisations we audit (audit risk) is absolutely central to our role and how we go about our audit work. However we, like the bodies we audit, are also subject to risk (business risk) and we need to have robust arrangements in place to manage those risks.

3. This document sets out our approach to risk management and outlines the key objectives, strategies, and responsibilities for the management of risk across the organisation. It applies to all Audit Scotland colleagues and should be applied consistently across the organisation. It will be supported by training and guidance to ensure that our colleagues are 'risk aware' but not 'risk averse'.

Overview of risk management

4. We are committed to achieving the aims defined in Public Audit in Scotland, our Corporate Plan and Business Group Business Plans. In so doing, we realise that we will face a variety of risks.

5. Risk is regarded as a quantifiable level of exposure to the threat of an event or action that could adversely affect our ability to achieve our objectives successfully. The task of management is to respond to these risks effectively so as to maximise the likelihood of Audit Scotland achieving its objectives and ensuring the best use of resources.

6. We use risk management to systematically identify, record, monitor and report risks to Audit Scotland to enable the organisation to meet its objectives and to plan actions to mitigate risks. There are five key aspects to our risk management process are illustrated in Exhibit 1.

Exhibit 1

Risk management process

Policy statement

7. We are committed to ensuring that the management of risk underpins all of our business activities and that robust risk management procedures are in place throughout the organisation. The application of this policy and strategy will enable us to identify, assess and respond to a changing risk profile.

8. We have a responsibility to manage risks and support a systematic approach to risk management including the promotion of a risk aware culture.

9. The application of risk management practices cannot and will not eliminate all risk exposure. Through the application of the risk management approach identified in this framework, we aim to achieve a better understanding of the risks faced by - and the implications for the business - and so inform our decision-making.

10. We recognise that risk, as well as posing a threat, also represents opportunities for developing innovative ways of working. There are also risks associated with not looking for, or taking, opportunities when they arise. Innovation and best practice should be shared across Audit Scotland and we want to be 'risk aware', but not 'risk averse'.

11. The importance of risk management is set out in the Corporate Plan and other supporting documentation such as Business Group Plans and risk registers.

12. We expect management to take action to manage and mitigate the effects of those risks that are considered to be in excess of Audit Scotland's risk appetite. Where a risk is deemed to be significant and/or in excess of Audit Scotland's risk appetite it will be highlighted in the Audit Scotland risk register along with the controls and actions being taken to mitigate the risk.

13. The active, ongoing commitment and full support of the Audit Scotland Board through the work of the Audit Committee and Audit Scotland Management Team is a necessary and essential part of this policy. Management will ensure that effective mechanisms are in place for assessing, monitoring and responding to any risks arising.

14. The corporate Performance and Risk Management Group acts as a 'Risk Forum'. Its role includes reviewing, challenging and agreeing which risks should be escalated for inclusion in the Audit Scotland risk register.

15. All colleagues are expected to have a good understanding of the nature of risk within Audit Scotland and the organisation's risk appetite. Also, those acting on behalf of Audit Scotland must accept responsibility for risks associated with their activities.

Risk management approach

Risk management objectives

16. The following objectives form the basis of our Risk Management framework:
    - Promote awareness of business risk and embed the approach to its management throughout the organisation.
    - Seek to identify, assess, control and report on any business risk that will undermine the delivery of Audit Scotland's business priorities, at a strategic and operational level.

Risk management vision

17. In order to achieve our vision of being a world class audit organisation we must have strong governance and management arrangements in place. Effective risk management is a core component of these arrangements.

18. We will identify the risk and its cause at the earliest opportunity; assess the potential impact on the organisation and put in place controls to mitigate the risk.

19. Additionally, we will seek to obtain assurance that the controls relied on to mitigate the key risks are effective. An assurance framework has been developed to support the ongoing monitoring of controls (see monitoring and reporting below).

Risk management culture

20. We recognise the values of an effective risk management culture. Systems and processes are dependent on the people operating and supporting them. They are also dependent on reflecting the environment within which they operate. Our approach to risk management therefore focuses on all of these aspects. We will:
    - review the corporate plan on an annual basis
    - review the Audit Scotland risk register and carry out risk interrogations on selected risks on a quarterly basis
    - integrate risk management with planning at strategic and operational levels
    - implement and monitor risk management arrangements across the organisation
    - welcome independent review of our arrangements, including internal and external audit
    - devolve responsibility for risk ownership and management as appropriate
    - ensure that designated individuals receive the necessary training, ongoing support and advice in connection with risk management
    - ensure that all colleagues understand our approach to, and their role in, risk management.

Risk management structure

21. To ensure that we have a full understanding of the risks we face and their implications risks will be identified and assessed at three levels:

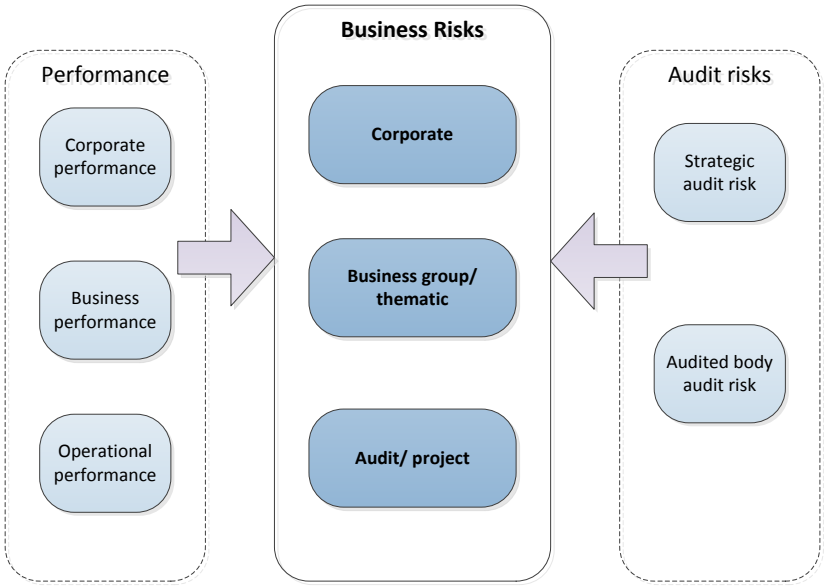
- **Corporate**: Those risks that, if realised, could have a significant detrimental effect on the Audit Scotland's key business processes and activities.
- **Business group and thematic:** Those business risks that, if realised, could have a significant detrimental effect on a Business Group's key objectives and activities. This also includes thematic risks, for example information risks monitored by the Knowledge, Information and Technology Governance Group (KITGG).
- **Project/ audit:** Those business risks that, if realised, could have a significant detrimental effect on the outcome of a project/ audit.

22. We will also use other elements of our management arrangements to inform our risk assessments (Exhibit 2). We will routinely consider how audit risks (i.e. those risks affecting audited bodies) identified though our audit risk management framework might impact on Audit Scotland.

23. We will also review risks in the context of our performance management arrangements to ensure that any issues identified through this route are reflected in risk registers. For example if performance reporting identified that audits were not running to schedule, or were over-budget we would assess the risk impact of this.

Exhibit 2

Risk management structure



Risk registers

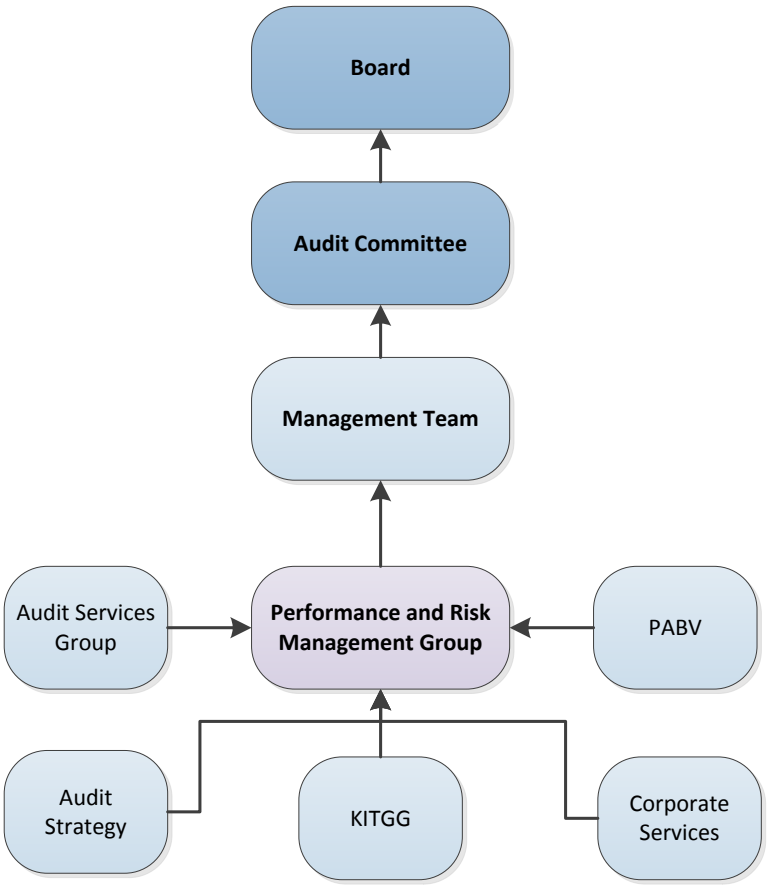
Audit Scotland's 'risk universe'

24. Risk registers are a key management tool. A risk register supports the identification, assessment and monitoring of risk. Risk registers also provide provides useful information on risk trends, action planning and offer a means of sharing of lessons / good practice across the organisation.

25. Audit Scotland's risk universe i.e. the level to which risks should be captured and recorded in risk registers is summarised in the Exhibit 3:

Exhibit 3

Risk management universe



Responsibilities

26. The Audit Scotland Board through its Audit Committee has ultimate responsibility for the management of risk.

27. The Accountable Officer has overall responsibility for risk management for Audit Scotland.

28. The Audit Scotland Management Team has day to day responsibility for the systems of internal control, including risk management. All staff should be risk aware. The key roles and responsibilities in relation to risk are summarised in Appendix 1.

29. The Audit Scotland Risk Register (ASRR) follows a standard format (Appendix 2) and includes the following elements:
    - gross risk assessments of likelihood and impact
    - active and monitoring controls in place to mitigate the gross risks
    - net risk assessments of likelihood and impact and any changes
    - further actions or monitoring required to reduce risk including; how the planned actions will manage the risk, timescales, action owners and risk review dates
    - target risk and target mitigation date
    - risk owner.

30. All other risk registers will follow the same format as the Audit Scotland risk register to ensure consistency across the organisation and facilitate risks being escalated, monitored and reported.

Risk registers

31. **Audit Scotland risk register**: This register reflects the most significant risks that have the potential to prevent Audit Scotland as a corporate body, from delivering its objectives set out in the Corporate Plan. The Audit Scotland's Management Team maintains and updates the risk register, with support from the corporate Performance and Risk Management Group (PRMG).

32. **Business group and thematic registers:** Business Groups maintain their own risk registers which reflect the specific risks associated with their activities. Any 'red' or 'amber' risks i.e. those which are significant, should be evaluated to decide whether they merit inclusion in the Audit Scotland risk register. This will be done through the PMRG. Nominated champions have responsibility for maintaining and updating risk registers in consultation with their business group management team.

33. **Audit/ project Risk Registers**: Separate risk registers are maintained for each major audit/ project. These cover significant pieces of core work and development projects. As with the business group risk registers risks should be assessed to determine whether they should be escalated to the business group register/ Audit Scotland risk register.

Risk management process

Risk identification

34. Risk identification is an ongoing activity, with individual risks and the impact and/or likelihood of risks materialising changing regularly. Risk identification is the process of determining what risks might prevent us from delivering our objectives, whether these are strategic or operational.

35. Risks can be triggered/ identified from a number of sources including:
    - changes to the operating environment/ periodic horizon scanning
    - planning (at strategic, business group and operational levels)
    - monitoring of audit risks (using the audit risk management framework)
    - monitoring of performance
    - existing forums (board, audit committee, management team, business group management teams, audit team/ project group meetings)
    - risks identified by internal/ external audit.

36. It is important, therefore, that risk features as a standing agenda item on management team meetings and working groups across Audit Scotland. Any risks identified should be reported for inclusion in the relevant risk register which would, in turn, be reviewed by a 'risk champion'.

37. Additional risk prompts/ tools are included as appendix 3.

Risk analysis and assessment

38. Once a risk is identified the risk is assessed. Risks should be assessed consistently across Audit Scotland considering – ***likelihood*** of the risk occurring, and if that risk was to occur, what the ***impact*** (i.e. consequences) on the organisation would be.

39. Likelihood will be categorised on a scale of 1 to 5 with one being rare and five almost certain. Impact will also be assessed on a scale of 1 to 5 with one being insignificant and 5 being severe. Likelihood and impact are multiplied together to obtain a total a gross risk score as illustrated in Exhibit 4.

Exhibit 4

Risk scoring

		LIKELIHOOD				
IMPACT	**Multiplier**	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
Multiplier		**1**	**2**	**3**	**4**	**5**
Severe	**5**	5	10	15	20	25
Major	**4**	4	8	12	16	20
Moderate	**3**	3	6	9	12	15
Minor	**2**	2	4	6	8	10
Insignificant	**1**	1	2	3	4	5

40. A table setting out what is meant by Insignificant, Minor, Moderate, Major and Severe classified by different types of events such as financial, regulatory, business continuity and reputational is included at Appendix 4.

Risk appetite

41. Risk appetite is an expression of how much risk Audit Scotland is prepared to take. Those involved in risk evaluation and prioritisation should, when considering risk, discuss and express the risk appetite as they see it.

42. The risk register format steers risk owners into considering risk appetite when updating a risk entry. They need to consider the risk score before and after existing mitigating action but also the final tolerable risk status (i.e. what they are aiming for in terms of status for that particular risk).

43. Audit Scotland's risk appetite is summarised in Exhibit 5.

Exhibit 5

Risk appetite

Risk Rating	Net risk assessment	Risk appetite response
High	**20 - 25**	Unacceptable level of risk exposure which requires action to be taken urgently. 'Red risks' at Business Group level should be included in the Audit Scotland risk register.
Medium	**12 - 16**	Acceptable level of risk but one which requires action and active monitoring to ensure risk exposure is reduced.
Low	**1 - 10**	Acceptable level of risk based on the operation of normal controls. In some cases it may be acceptable for no mitigating action to be taken e.g. net risk< 4.

Risk response

45. Based on risk scores there are four response options:

- **Terminate** - in this situation the risk is terminated by deciding not to proceed with an activity. For example, if a particular project is very high risk and the risk cannot be mitigated it might be decided to cancel the project. Alternatively, the decision may be made to carry out the activity in a different way.
- **Transfer** - in this scenario, another party bears or shares all or part of the risk. For example, this could include transferring out an area of work or by using insurance.
- **Treat** - this involves identifying mitigating actions or controls to reduce risk. These controls should be monitored on a regular basis to ensure that they are effective.
- **Tolerate** - in this case, it may not always may be necessary (or appropriate) to take action to treat risks, for example, where the cost of treating the risk is considered to outweigh the potential benefits. If the risk is shown as 'green' after existing mitigating actions then it can probably be tolerated.

Risk mitigation

46. These are the controls and actions put in place to reduce the likelihood the risk occurring, or minimise the impact of the risk if it does occur. An internal control system incorporating policies, processes, business continuity arrangements and other aspects of Audit Scotland's operations should, when taken together:

- enable the organisation to respond appropriately to business risks
- help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate the flow of timely, relevant and reliable information, and
- help ensure compliance with applicable laws and regulations, and also with internal policies. This would include, for example, having formal written procedures and policies applied consistently across the organisation supported by training for staff.

47. The residual risk which remains after taking account of the relevant mitigations is the net risk. It is also good practice to define 'target' risk which, in simple terms, is the tolerable level of risk that the organisation should aim for.

48. The risk register format requires active and monitoring controls to be identified to inform the net risk assessment. The risk register also prompts for additional actions where the net risk is above the target risk.

Risk escalation

49. This is a process which ensures that significant risks are escalated to the appropriate person or group. This is necessary to ensure the appropriate decisions and/or actions are implemented to mitigate the risk.

50. It is key to the risk escalation process that risk information is made available to the right people in a timely way. There is no restriction on what may be escalated for action, however the key criteria is that some form of intervention is required from more senior management.

51. It is the responsibility of individual risk owners to raise risks which they believe require action by a higher authority. It should be emphasised though that we want to discourage people from escalating risks that they should dealing with themselves. High risk issues should be escalated through the hierarchy that makes up the risk universe so that they are captured in the appropriate register for information purposes. However, responsibility for addressing the risk may still remain with the originator.

52. Risks should feature as a standard agenda item at management and working group meetings. Discussions on risk should include:
    - new or emerging issues and risks
    - evaluation and criticality of new or emerging issues and risks
    - decisions required and by whom
    - mitigating actions, action owners, timescales and review points
    - ownerships of new risks
    - review of existing risks and the effectiveness of the current controls in place

53. Risks should be discussed, evaluated and escalated upwards, as appropriate, through the risk universe to ensure that the most significant risks (and mitigating actions) are reflected in the appropriate risk register.

Monitoring and reporting arrangements

Monitoring risks

54. Risk management is an ongoing process that needs to be embedded in everyday activity. The process must be reviewed on a regular basis to remain effective. It is the responsibility, therefore, of each risk owner to review risks on a regular basis and identify whether any revisions are required. The revision may involve a re-assessment of impact and likelihood or planned mitigating actions.

55. As previously stated, it is important that risk is included as a standing item on the agenda for management teams (at all levels within the organisation) and working groups so that risks can be identified and captured. As a minimum, on a quarterly basis each Director will seek assurance from individual risk champions that the risks in their assigned areas are being adequately monitored and action is being completed as agreed in formal action plans.

56. Through the risk champions and the Performance & Risk Management Group (PRMG) risks will be reviewed on a quarterly basis, including a review of the high risks facing Audit Scotland and mitigating action plans. This group will link directly with the Audit Scotland Management Team and will advise them on which risks to escalate / de-escalate for inclusion or deletion from the Audit Scotland risk register.

Action planning

57. In situations where a risk is classified as 'to be treated', and scores either 'amber' or 'red' then an action plan needs to be prepared. The action plan is the mechanism whereby:
    - the risk owner records the actions to be taken
    - the controls that need to be put in place / strengthened
    - the action owner, and
    - the timescale for implementation.

58. Additionally, the action plan should indicate whether planned actions are aimed at reducing the likelihood and / or the impact of the risk. Action updates should be provided at least quarterly to the 'risk champions' so that they can advise the Performance and Risk Management Group (PRMG) of any changes in the risk profile. The PRMG in turn would update the Audit Scotland risk register for the Audit Scotland Management Team to consider and approve, including any additional actions required to further reduce risks.

Reporting and assurance arrangements

59. Audit Scotland's risk management framework will be supported through agreed reporting and assurance arrangements. This is to ensure that the key risks and their owners are clearly identified that mitigation and specified actions are appropriate and that actions are being carried out. The arrangements, include:

Corporate level

60. Audit Scotland's Board will review and approve risk management policies and strategies. It will take advice from the Audit Committee on these matters.

61. On a routine basis the Audit Committee will receive updates on Audit Scotland's risk management framework and risks. Reporting will include:

- the risk management framework and Audit Scotland's approach to risk
- the Audit Scotland Risk Register including associated action plans for the higher rated risks, and
- reports on the changing risk profile within Audit Scotland including areas of increasing risk, where controls are not considered to be effective and horizon scanning for areas of possible future risk.

62. The Audit Committee will also review the Audit Scotland Risk Register at each meeting and will receive an annual report on risk management from the internal auditors. The committee will also consider input from other sources of assurance as appropriate.

63. The Audit Committee also considers a detailed risk interrogation of one of the identified risks at its meetings.

64. In its annual written report to Audit Scotland's Board, the Audit Committee will include its review of risk management and an updated version of the Audit Scotland Risk Register.

65. The Audit Scotland Management Team (ASMT) will maintain and regularly review (and update) the Audit Scotland Risk Register of the key risks facing the organisation. The ASMT while retaining ultimate responsibility for updating the Audit Scotland risk register will delegate the detailed review work to the PRMG.

Business Group level

66. Each Director / Head of a Business Group will review risks and actions in mitigation of risk on a regular basis as an integral part of the business planning process. These officers will also ensure that risks identified at a Business Group level and which may have a wider impact on the organisation are escalated through the risk universe, via risk champions initially.

67. Risk champions in each Business Group play a key role in the risk management process. They are responsible for identifying and escalating those high risks that should be considered by PRMG for inclusion in the Audit Scotland risk register. Risk champions in conjunction with

their local Business Group management teams should review on a quarterly basis and consider:

- the status of all high risks (including actions taken)
- any new risks since the last report
- changed risks from the previous report (especially where risk is increasing)
- risks escalated from Business Group / Information / Public Sector registers to the Audit Scotland Risk Register; and
- risks removed from registers.

68. The PRMG, after considering feedback from risk champions, will update the Audit Scotland risk register and provide the Audit Scotland Management Team with an overview of the risk profile across Audit Scotland

Audit/ project level

69. Risks associated with audits/ projects will be reviewed by the manager/ project sponsor or officer responsible for maintaining the project risk register depending on delegated authority. Risks identified in audit/ project risk registers will be reviewed and considered by the relevant the Business Group and will feature as part of the overall review of business group risk register.

Risk management maturity model

70. A key aspect of monitoring and reporting progress is the establishment of a Risk Maturity Model. This model provides senior management with a snapshot of where the risk processes and principles Audit Scotland employs have led to changes and progression in risk management. It provides assurance that risk management processes are fit for purpose and also identifies areas where further improvement is required. Audit Scotland's risk maturity model is attached as Appendix 5.

71. The risk maturity model will be reviewed annually by internal audit with findings discussed by the Audit Scotland Management Team (via the PRMG). The Management Team would then propose any actions to raise 'maturity' in areas of poorer performance for consideration by the Audit Committee and subsequent approval by the Audit Scotland Board.

Appendix 1: Responsibilities

Level	Role & responsibilities	Frequency
Senior Management		
Audit Scotland Board	• Setting the tone at the top for risk management throughout the organisation • Approving the overall risk management arrangements including the appetite for risk • Considering reports on the operation of risk management arrangements via reports from the Audit Committee, the Accountable Officer and through consideration of the annual assurances for the completion of the annual report and accounts.	Annually
Audit Committee	• Scrutinising Audit Scotland's risk management framework • Reviewing the strategic processes for risk, control and governance (including the Accountable Officer's Governance Statement) • Monitoring the effectiveness of risk management arrangements • Scrutinising Audit Scotland's approach to risk tolerance (i.e. risk appetite) • Review the Audit Scotland risk register • Review the scheduled risk interrogation.	Annually At each quarterly meeting
Accountable officer	• Specific personal responsibility for signing the annual accounts including the Accountable Officer's Governance Statement.	Annually
Audit Scotland Management Team (ASMT)	• Owners of the Audit Scotland risk register and are responsible for ensuring its completeness and accuracy • Conducting scheduled risk interrogations • Reviewing and challenging 'red' (high) risks • Ensuring that there is ownership for all significant risks by a member of the ASMT • Approving and recommending to Audit	Quarterly As required

Level	Role & responsibilities	Frequency
	Committee draft risk policies & strategies • Determining Audit Scotland's overall approach to risk and risk tolerance • Reviewing corporate risks including response approach (Terminate /Transfer/Tolerate /Treat) • Preparing corporate business plans incorporating risks and planned mitigating actions • Reviewing risk maturity model	
Directors and Assistant Directors	• Risk owners for specified risks • Responsible for implementing the risk policy, strategy and assurance framework within their areas of responsibility and accountability • Fostering a culture of risk management and risk awareness • Preparing business plans incorporating risks and planned mitigating actions • Ensuring that all identified risks are captured in the relevant risk register and Business Group Register where appropriate • Actively manage risks through identification of mitigating controls, taking action and regularly discussing and reporting on risks • Nominating and appointing 'risk champions to co-ordinate risk management activity within their areas of responsibility • Risk being a standing item on management meetings.	Ongoing
Risk Forum & Risk Champions		
Performance & Risk Management Group (PRMG)	• Contribute to and review the Audit Scotland risk register, including: – testing the content against the risk prompts – testing content against audit risk and performance reports • Reviewing and challenging 'red'(high) risks based on management information: trends, horizon scanning, areas of increasing risks,	Quarterly

Level	Role & responsibilities	Frequency
	risks where controls are not effective • Challenging progress against risk action plans holding those to account for agreed actions • Liaising with 'risk champions' to identify possible corporate risks • Advising the ASMT on risks to be escalated for inclusion in the Audit Scotland risk register • Challenging risk registers in relation to the identification of risk, the assessment of risk and proposed mitigating actions • Ensuring proper follow-action actions are being implemented where risk exposure remains high despite mitigating controls • Providing training to staff supported by risk champions.	Ongoing
Risk champions (Senior staff nominated by their Director to support and be integral to the risk management framework)	• Supporting Audit Scotland's risk management framework • Being a key reference point for staff in providing support and advice on risk management • Maintaining and updating business group risk registers • Working with other risk champions to ensure consistency of approach across the organisation • Challenging risk owners in relation to the identification of risk, the assessment of risk and proposed mitigating actions and action plans • Actively supporting PRMG by advising on risks to escalate for inclusion in the Audit Scotland risk register.	Ongoing
Other staff		
Risk owner - the designated individual to manage and monitor risks. (For risks included in Audit Scotland risk register this must be a Director).	• Maintaining all aspects of risk assigned to them including the actions needed to mitigate risk and maintaining an action plan • Obtaining senior management support where necessary (e.g. deciding on target risk • Liaising with 'risk champions' to ensure that	Ongoing

Level	Role & responsibilities	Frequency
	risk registers are kept up to date • Escalating risks where appropriate	
Working groups	• Ensuring that risks is appropriately considered at meetings and minuted • Facilitate the sharing of best practice and lessons learnt.	Per timetabled meetings
Colleagues	• Following Audit Scotland's risk management framework (including firms appointed by AS). • Understanding risk and being aware of the role of risk owners & risk champions • Good understanding of the part they play in delivering Audit Scotland's risk management framework • Being risk aware and reporting potential risks to line management for consideration.	Ongoing
Internal audit		
Internal audit	• Internal audit work is undertaken on the major risks faced by the organisation and the effectiveness of associated controls is assessed. • Independent assurance is provided more generally on the management of risk.	Part of annual audit programme of work

Appendix 2: Risk register format

	Risk description	Gross risk			Controls in place	Net risk			Prev. net risk / change	Planned actions, owners and timescales	Target Risk & mitigation date	Risk Owner
		L	I	Tot		L	I	Tot				
	Vision : To be a world class audit organisation that improves the use of public money											
1.	**Failure to deliver our vision** We do not deliver on our vision to be world class audit organisation that improves the use of public money.	3	5	15	***Active controls:*** - Board, MT, LG - External engagement by AC, AGS, CoA and AS - Engagement with SCPA - Strategic plans (Public Audit in Scotland, AC strategy, Corporate plan). ***Monitoring controls:*** - Annual reports - Quarterly performance & BWC reporting	2	4	8	8 ⇨	**Actions** - BWC programme 2015-18 - Corporate Plan update 2016 (DM) **Objectives** BWC improvement programme and corporate plan identify improvement objectives to deliver the vision. **Review** Annual Reports 2015/16	4 31/03/17	CG

Notes

- All risk register should follow the same format as the Audit Scotland risk register
- Gross and net risk scores should be colour coded in accordance with Audit Scotland's risk scoring matrix
- High ('red') net risks should be escalated for inclusion in the Audit Scotland risk register, as appropriate
- Net risk from the previous review period should included in the register for monitoring purposes
- The change in risk profile from one period should be backed up by detailed notes
- Target risk is the level of tolerable risk where no further mitigating actions are required
- The risk register is intended to be a dynamic document reflecting the fact that risks may change between formal reviews. The register will be updated between reviews to reflect changes in risks as they are identified.

Appendix 3 - Risk prompts and tools

Many risk prompts and tools exist and risks are most likely to be identified where different tools are adopted based on the circumstances.

Some options are covered below and the PMRG will develop further guidance as required.

Environmental scanning approaches

Using established tools including

- PESTLE analysis (**P**olitical, **E**conomic, **S**ocial, **T**echnological, **L**egal, **E**nvironmental
- SWOT analysis (**S**trengths, **W**eaknesses, **O**pportunities, **T**hreats)

Process based approach

- Input risks; including - financial, employees, assets, ICT
- Process risks; including - management processes, methodology
- Output risks; including - quality, timeliness, relevance, demand
- Outcome risks; including - impact, effectiveness, reputation.

Prince2 prompts

- Strategic/ commercial risks
- Economic/ financial/ market risks
- Legal and regulatory risks
- Technical/ operational/ infrastructure
- Organisational/ management/ human factors
- Political factors
- Environmental factors

Corporate strategy prompts

Is there a risk of……..

Vision : To be a world class audit organisation that improves the use of public money
Failure of vision - We do not have a clear vision for the organisation
Failure of shared vision - Divergence of views on direction amongst; AGS, AC, AS, Board, Scottish Parliament, Audited bodies
Failure to deliver our vision - We do not deliver on the objectives contained in our vision
Failure of legitimacy - Our vision is not shared by key stakeholders
Failure of independence - A real/ perceived lack of independence and/or impartiality undermines the impact/value of our work
Failure of relevance - We are unable to manage changing stakeholder expectations effectively leading to a decline in relevance
Failure of reputation - Failure of quality, independence, impact, missed issue, governance or resource management results in damage to credibility, particularly in heightened political climate
Failure of clarity - Lack of understanding about the respective roles of AC, AGS, AS amongst stakeholders
What we do: Helping to improve by holding to account: auditing, reporting, recommending actions
Failure of focus and scope - Our audits focus on the wrong issues, are not timely or miss a significant issue
Failure of quality - We do not deliver quality work leading to reduced confidence and impact.
Failure of impact and influence - Audits do not lead to improvement
Failure of innovation - We fail to innovate and improve, or innovation and improvement are not subject to appropriate control
Failure of capacity - We are unable to meet the demand for audit under the new financial powers and fiscal framework

Failure of process - Our audit work is not carried out in accordance with procedures
Failure of communication (external) - Our messages are not clear to stakeholders (inc audit reports and other corporate communications)
How we do it: Quality & Impact, Knowledge Management, Innovation, Value for Money, Valuing People, One Organisation
Failure to achieve value for money - We fail to achieve or demonstrate value for money
Failure to operate as one organisation - We fail to work effectively across the organisation leading to fragmented impact, mixed messages and inefficiency
Failure of culture - Our culture does not support our vision of becoming work class
Failure of governance - Our governance arrangements fail to manage business effectively
Failure of communication (internal) - Our internal communication arrangements fail to manage communications effectively
Failure of resourcing (people) - We fail to recruit, retain, develop and motivate people with skills we need to do our work leading to reduced quality of our work
Failure of resourcing (people) - Capacity (numbers), Capacity (skills), Recruitment (market impact), selection, induction, skills, training and development, performance management, departure, succession planning
Failure of resourcing (financial) - Budget planning, Budget management, Procurement, Payment
Failure of resourcing (assets) - Edinburgh office move, office availability
Failure of resourcing (ICT) - Systems loss, data loss
Failure of process (performance management) - Our performance management arrangements fail to support us effectively
Failure of process (risk management) Our risk management arrangements fail to identify and manage risk effectively

Appendix 4 - Risk impact descriptions

Description	Financial	Injury or Illness	Asset Loss	Business Continuity	Reputational	Corporate Objectives	Regulatory & Legal
Insignificant	<£50k	Minor injury, or illness, first aid, no days lost	Minor damage to single asset	<0.5 days	Minor media interest	<2.5% variance	Act or Omission resulting in Legal or Regulatory breach causing insignificant impact loss (as categorised in other six impact categories)
Minor	£50k – 100K	Minor injury, or illness, medical treatment, days lost	Minor damage to multiple assets	0.5>1 day	Headline media interest	2.5-5% variance	As above Causing minor loss
Moderate	£0.1>0.25 m	Moderate injury, medical treatment, hospitalisation, <14 days lost, RIDDOR reportable	Major damage to single or multiple assets	1>7 days	Headline media interest causing public embarrassment	5-10% variance	As above Causing moderate loss
Major	£0.25m> 0.5m	Single death, extensive injuries, long-term illness (>14 days)	Significant loss of assets	7>30 days	Short-term media campaign	10-25% variance	As above Causing major loss
Severe	>£0.5m	Multiple deaths or severe disabilities	Complete loss of assets	>30 days	Sustained media campaign/ lobbying	>25% variance	As above Causing catastrophic loss and Legal or

Description	Financial	Injury or Illness	Asset Loss	Business Continuity	Reputational	Corporate Objectives	Regulatory & Legal
							regulatory supervision

Appendix 5 - Risk maturity model

	Risk Governance	Risk identification & assessment	Risk mitigation & treatment	Risk reporting & review	Continuous improvement
Enabled	Risk management and internal control is fully embedded into operations. All parties play their part and have a share of accountability for managing risk in line with their responsibility for the achievement of objectives.	There are processes for identifying and assessing risks and opportunities on a continuous basis. Risks are assessed to ensure consensus about the appropriate level of control, monitoring and reporting to carry out. Risk information is documented in a risk register.	Responses to the risks have been selected and implemented. There are processes for evaluation risks and responses implemented. The level of residual risk after applying mitigating controls is accepted by the organisation, or further mitigations have been planned.	High quality, accurate and timely information is available to operational management and directors. The board reviews the risk management strategy, policy and approach on a regular basis e.g. annually, and review key risks, emergent & new risks, and action plans on a regular basis.	The organisational performance management framework and reward structure drives improvements in risk management. Risk management is a management competency. Management assurance is provided on the effectiveness of their risk management on a regular basis.
Managed	Risk management objectives are defined & managers are trained in risk management techniques. Risk management is written into performance	There are clear links between objectives and risks at all levels. Risk information is documented in a risk register. The organisation's risk	There is clarity over the risk level that is accepted within the organisation's risk appetite. Risk responses are appropriate to satisfy the risk appetite of the	The board reviews key risks, emergent and new risks, and action plans on a regular basis. It reviews the risk management strategy, policy and approach on a regular	The organisation's risk management approach and the Board's risk appetite are regularly reviewed and refined in light of new risk information reported.

	Risk Governance	Risk identification & assessment	Risk mitigation & treatment	Risk reporting & review	Continuous improvement
	expectations of managers. Management and executive level of responsibilities for key risks have been allocated.	appetite is used in the scoring system for assessing risks. All significant projects are routinely assessed for risk.	organisation have been selected and implemented.	basis (annually). Directors require interim updates from delegated managers on individual risks which they have personal responsibility.	Management assurance is provided on the effectiveness of their risk management on an ad hoc basis. The resources used in risk management are become quantifiably cost effective. KPIs are set to improve certain aspects of risk management activity e.g. number of risks materialising or surpassing impact – likelihood expectations.
Defined	A risk strategy and policies are in place and communicated. The level of risk taking that the organisation will accept is defined and understood in some parts of the organisation, and it is used to consider the	There are processes for identifying and assessing risks and opportunities in some parts of the organisation but not consistently applied in all. All risks identified have been assessed with a defined scoring system. Risk	Management in some parts of the organisation are familiar with, and able to distinguish between, the different options available in responding to risks to select the best response in the interest of the organisation.	Management have set up methods o monitor the proper operation of key processes, responses, and actions plans. Management report risks to directors where responses have not managed the risks to a level acceptable to the	The Board gets minimal assurance on the effectiveness of risk management.

	Risk Governance	Risk identification & assessment	Risk mitigation & treatment	Risk reporting & review	Continuous improvement
	most appropriate responses to the management of identified risks. Management and executive level of responsibilities for key risks have been allocated.	information is brought together for some parts of the organisation. Most projects are assessed for risk.		board.	
Aware	There is a scattered, silo-based approach to risk management. The vision, commitment and ownership of risk management have been documented. However, the organisation is reliant on a few people for the knowledge, skills and the practice of risk management activities on a day-to-day basis.	A limited number of managers are trained in risk management techniques. There are processes for identifying and assessing risks and opportunities, but these are not fully comprehensive or implemented. There is no consistent scoring system for assessing risks. Risk information is not fully documented.	Some responses to the risks have been selected and implemented by management according to their own perception of risk appetite in the absence of a board-approved appetite for risk.	There are some monitoring processes and ad hoc reviews by some managers on risk management activities.	Management does not assure the Board on the effectiveness of risk management.

	Risk Governance	Risk identification & assessment	Risk mitigation & treatment	Risk reporting & review	Continuous improvement
Naive	No formal approach developed for risk management. No formal consideration of risks to business objectives, or clear ownership, accountability and responsibility for the management of key risks.	Processes for identifying and evaluating risks and responses are not defined. Risks have not been identified nor collated. There is no consistent scoring system for assessing risks.	Responses to the risks have not been designed or implemented.	There are no monitoring processes or regular reviews of risk management.	Management does not assure the Board on the effectiveness of risk management.

Source: Internal audit report on Risk Management (January 2014

Item: 15
Board: 05/2016

AUDIT SCOTLAND BOARD

3 MAY 2016

REPORT BY THE ASSISTANT DIRECTOR, CORPORATE PERFORMANCE AND RISK

DRAFT INFORMATION SECURITY MANAGEMENT POLICY

1. Purpose of Report

This report invites the Board to approve a revised Information Security Management Policy.

2. Background

The Board approved the Information Services Strategy at its meeting on 17 September 2015. The strategy set out how we are using information technology to support our aim of being a world class audit organisation.

At the same meeting the Board re-approved the Data Protection, Freedom of Information, Records Management and Information Security policies for a further year. The Board also noted that Management Team had requested review be undertaken of our policies and our process for managing them to:

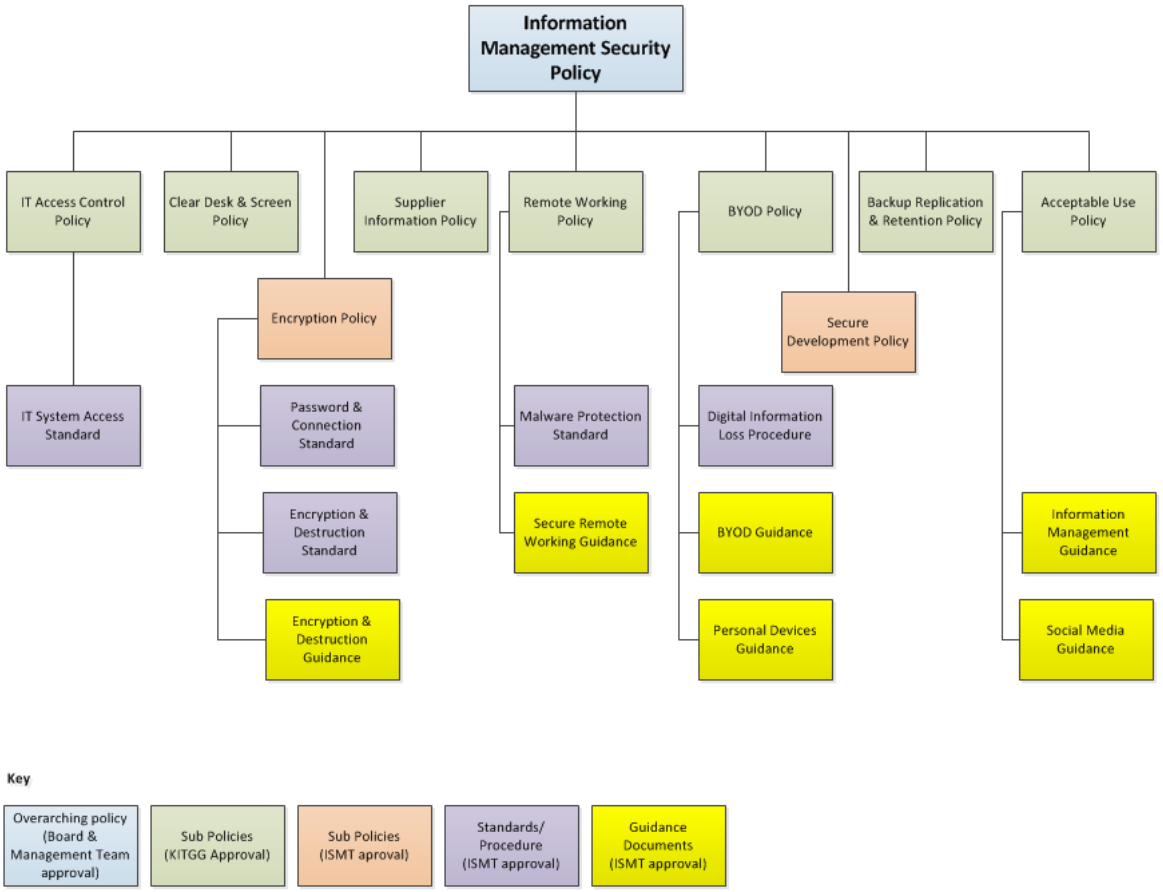
- rationalise, consolidate and simplify the policies wherever possible
- ensure that they are consistent with the culture of empowering and enabling colleagues to work in a flexible way, while retaining the appropriate safeguards, and ensure that this is reflected the tone and language of the policies
- rationalise and enhance 'user friendly' guidance to support the practical implementation of the policies where required
- review the frequency, ownership and authorising environment is appropriate and fit for purpose.

In parallel we are working to achieve ISO 27001:2013 Information Security certification. To achieve certification we must successfully complete two external audits. The first 'stage 1 audit' on 9th May 2016 will review the Information Security Management System documentation and the second 'stage 2' audit, scheduled approximately 12 weeks later (date confirmed following successful Stage 1 audit) will be a more detailed audit to test that our policies and procedures are working in practice.

3. The information security management system

The Information Security Management System (ISMS) comprises of policies, procedures and standards that support world class information security. These

documents are structured in a hierarchical manner and devolve responsibility as shown in diagram below.



The attached Information Security Management Policy is overarching policy for the ISMS. It sets out the overarching principles of information security and the associated roles and responsibilities. All other information security sub-policies, procedures and standards are controlled by this policy and derive responsibility from it. Each level of responsibility must report any policy exceptions and non conformity to its oversight group.

The ISMS and the Information Security Management Policy were reviewed and agreed by Management Team at its meeting on 12 April 2016.

4. Recommendation

The Board is invited to:

- note the ISMS structure and
- review and approve the Information Security Management Policy

Information Security Management Policy

Version:	1.2	Status:	Approved by Management Team (pending Board approval)
Author/Owner:	IT Manager	Approval/Review:	Management Team and Board
Approval Date:	12 April 2016	Review Date:	3 May 2017

Introduction

1. This policy sets out Audit Scotland's strategic commitment to Information Security Management.
2. Audit Scotland will ensure the confidentiality, integrity, quality and availability of all the information it holds and processes.
3. Audit Scotland will ensure all the information it holds and processes will meet its contractual, legal and regulatory obligations.

Scope

4. This policy is mandatory for all employees, contractors and consultants employed by Audit Scotland. Failure to comply with this policy and supporting information security policies may result in disciplinary action or contract termination.

Commitments

5. Audit Scotland will take appropriate action to ensure the confidentiality, integrity and quality of all the information it holds and processes.
6. Audit Scotland will produce, maintain and test business continuity plans to ensure the availability of its information and information systems.
7. Audit Scotland will treat information security as a business critical issue.
8. Audit Scotland will ensure that its information is open and not restricted by financial or legal agreements.
9. Audit Scotland will ensure legislative and regulatory requirements are met (including intellectual property rights).

10. Audit Scotland will identify and implement appropriate controls for information assets proportionate to levels of risk.

11. Audit Scotland will communicate all appropriate information security policies to all employees, contractors, consultants, clients and other stakeholders.

12. Audit Scotland will allocate individual accountability for compliance with all appropriate information security policies, standards, guidance and procedures.

13. Audit Scotland will continue to improve its information security management.

14. Audit Scotland will develop, implement and maintain an Information Security Management System (ISMS) in accordance with the best practice contained within ISO/IEC 27001:2013 and ISO/IEC 27002:2013.

Responsibilities

15. Audit Scotland's Board through its Audit Committee has oversight of risks, including information risks.

16. Audit Scotland's Accountable Officer, with support from the Management Team, has overall responsibility for ensuring this policy is effectively implemented and delivered.

17. Audit Scotland's Senior Information Risk Officer is the Chief Operating Officer, who is responsible for the overall management of the organisation's information risks.

18. Audit Scotland's Management Team will implement and manage appropriate controls to enable conformance to information security policies within their own areas of responsibility and will ensure individual accountability for control performance.

19. The Knowledge, Information and Technology Governance Group (KITGG) will support the Accountable Officer, Senior Information Risk Officer and Management Team by assessing and mitigating information security risks and providing assurance.

20. The KITGG will maintain this policy and associated information security policies ensuring they are communicated, reviewed and updated in response to changes in risks faced by Audit Scotland, legislation, and internal operational working practices.

21. The KITGG will ensure all information security policies and our performance in meeting their requirements is monitored and reviewed on an annual basis.

22. The Information Services Management Team (ISMT) will maintain information security standards, guidance and procedures ensuring they are communicated, reviewed and updated in response to changes in risks faced by Audit Scotland, legislation, and internal operational working practices.

23. The Corporate Governance Manager is responsible for updating Audit Scotland's data protection notification, managing data subject access requests and providing advice to staff.

24. Information Asset Owners must understand the information held by their business area, and approve the permissions required to access it.

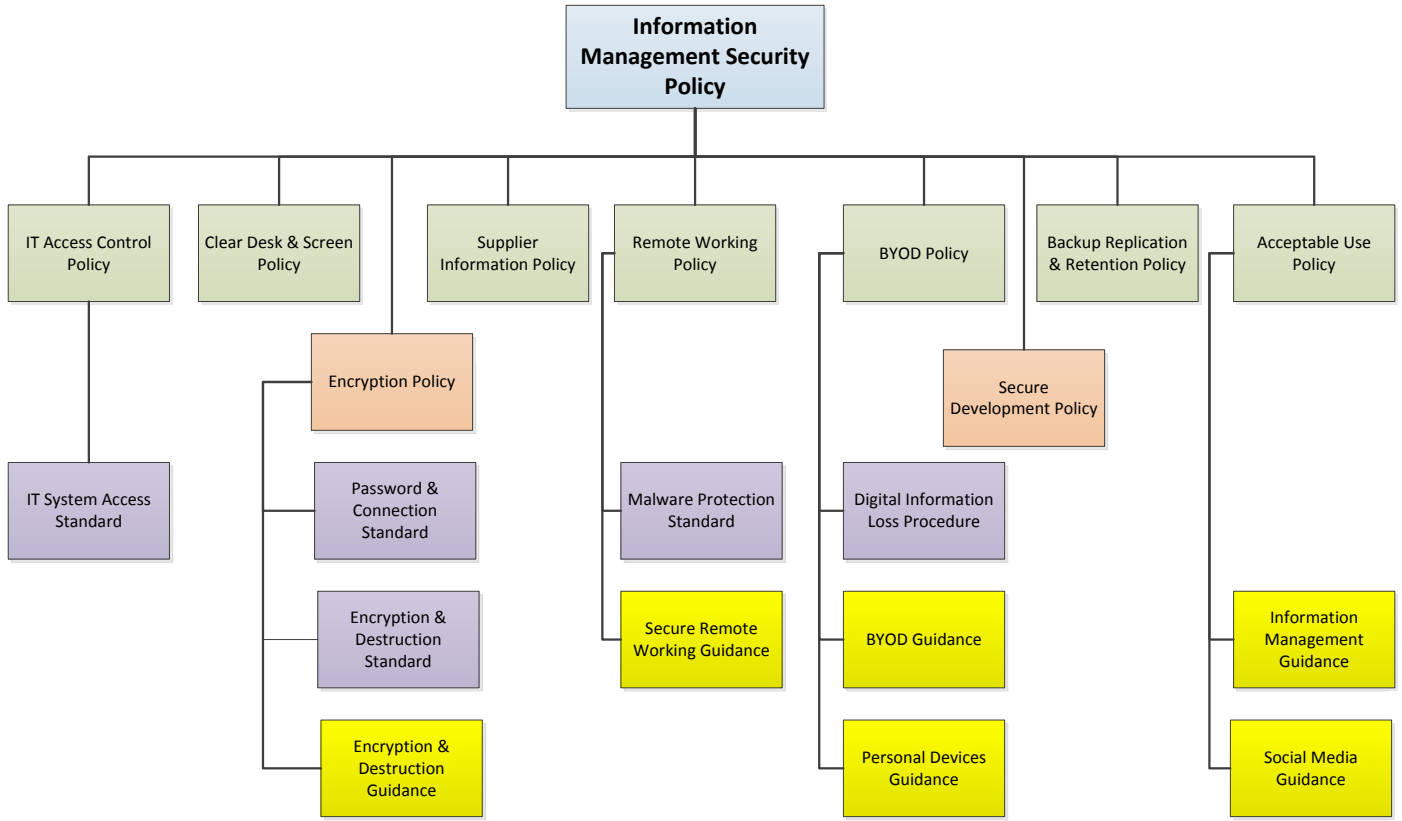
25. All Managers will be responsible for implementing and communicating appropriate information security policies, guidance and procedures.

26. All employees, contractors and consultants employed by Audit Scotland are required to play an active role in the protection of company assets and treat information security appropriately in order that this purpose can be achieved.

Change Log

Version	Date	Author	Description
1.0	22/03/16	IT Manager	Information Security Management policy drafted for KITGG approval.
1.1	05/04/16	IT Manager	Some minor changes suggested by the KITGG and policy approved. For submission to the Audit Scotland Management Team for approval.
1.2	15/04/16	IT Manager	Minor changes to reflect Audit Management Team comments. Approved by Management Team and for submission to the Audit Scotland Board.

Appendix 1


Information Management Security Policy
IT Access Control Policy
Clear Desk & Screen Policy
Supplier Information Policy
Remote Working Policy
BYOD Policy
Backup Replication & Retention Policy
Acceptable Use Policy
Encryption Policy
Secure Development Policy
IT System Access Standard
Password & Connection Standard
Malware Protection Standard
Digital Information Loss Procedure
Encryption & Destruction Standard
Secure Remote Working Guidance
BYOD Guidance
Information Management Guidance
Encryption & Destruction Guidance
Personal Devices Guidance
Social Media Guidance
Key
Overarching policy (Board & Management Team approval)
Sub Policies (KITGG Approval)
Sub Policies (ISMT aproval)
Standards/ Procedure (ISMT approval)
Guidance Documents (ISMT approval)

Item: 16
Board: 05/2016

AUDIT SCOTLAND BOARD

3 MAY 2016

REPORT BY THE ASSISTANT DIRECTOR, CORPORATE PERFORMANCE AND RISK

PUBLICATION OF BOARD PAPERS

1. Purpose of report

This paper provides guidance for Board members on the publication of papers.

2. Background

At its meeting on 26 February the Board considered a report on options to support greater openness and transparency. The Board agreed that Board papers should be published on the Audit Scotland website in addition to the agendas and minutes.

At its meeting on 24 March the Board considered the process for determining public and private papers, guidance to support this and the arrangements to support the publication process.

The draft minute of the meeting notes that members 'agreed to implement the new arrangements with effect from the papers for the May 2016 meeting. Members also agreed that the effectiveness of the arrangements should be reviewed after six months'.

The working assumption is that the majority of Board papers will be public. However there may be some instances where it is appropriate that papers will be private. The main categories where papers may be considered private are:

- statutory/security/legal
- commercial sensitivity
- effective conduct of business.

3. Public and private papers - guidance

Appendix 1 to this report is a short summary of the categories where papers may be considered private.

Appendix 2 to this report is the more detailed guidance agreed by the Board at its last meeting.

4. Recommendation

The Board is invited to use the attached guidance to help inform its determination of public and private papers.

Summary guidance on publication of Board papers

1. In February 2016 the Audit Scotland Board agreed that board papers should be published on the Audit Scotland website alongside the agenda and minutes of the meetings. The Board agreed additional guidance on this at its meeting on 24 March 2016.

2. This guidance offers advice on determining which papers are appropriate for publication.

3. The presumption is that Board papers will be public unless they contain information which falls into one of the following categories:

    - Statutory/ security/ legal: including
        - Personal information
        - Danger to health and safety
        - Danger to security
        - Prohibitions on disclosure
        - Legally privileged information
        - Information provided in confidence
    - Commercial sensitivity
    - Effective conduct of business: including:
        - Prejudicing the free and frank provision of advice/ exchange of views for the purposes of deliberation/ conduct of public affairs
        - Information intended for future publication

4. Even in these circumstances papers may be published subject to specific redactions from the text.

5. The detailed guidance is available here.

Board papers

Guidance

AUDIT SCOTLAND

Prepared for Colleagues
March 2016

Audit Scotland is a statutory body set up in April 2000 under the Public Finance and Accountability (Scotland) Act 2000. We help the Auditor General for Scotland and the Accounts Commission check that organisations spending public money use it properly, efficiently and effectively**.**

Contents

Introduction

Background

1. Openness and transparency are fundamental to effective governance and are guiding principles in our Corporate Plan, where we state 'We expect high standards of governance of the organisations we audit and we set high standards for our own governance. We believe that a world-class organisation requires world-class governance arrangements'.

2. In February 2016 the Audit Scotland Board agreed that board papers should be published on the Audit Scotland website alongside the agenda and minutes of the meetings. The Board agreed additional guidance on this at its meeting on 24 March 2016.

3. This guidance offers advice on determining which papers are appropriate for publication.

4. The presumption is that Board papers will be public unless they contain information which falls into one of the following categories:
   - Statutory/ security/ legal
   - Commercial sensitivity
   - Effective conduct of business

5. Even in these circumstances papers may be published subject to specific redactions from the text.

General guidance

6. Audit Scotland has a long standing commitment to clear and concise reporting and reports and other papers should be written in plain and easy to understand language. Further guidance can be found in the A-Z style guide.

7. Board papers should be prepared on the presumption that they will be published and this should be reflected in the tone and content of the report when authors are preparing them.

8. In addition, papers must be supplied in a timely fashion in advance of Board meetings to provide for quality assurance checking. Papers should therefore be supplied one week in advance of the issue date i.e. **two weeks in advance of the Board meeting date** (See appendix).

9. If a report author considers that a report should be a private paper they should bring this to the attention of the Chief Operating Officer along with an explanation of why this should be the case (with reference to the criteria set out below).

10. At the end of its meeting the Board will be invited to confirm which of the papers should be classified as private and the reason for this. This will be reflected in the Board minutes.

11. Board papers will then be published on the website alongside the relevant agenda and minutes when the minute has been agreed by the Board.

Guidance on public and private papers

Introduction

12. We have developed a range of criteria to inform decisions on whether a paper should be private. We used the Freedom of Information (Scotland) Act 2002[1] (FOISA) as a starting point, the logic being that the act presumes openness but also recognises some instances where a degree of privacy is appropriate.

13. The criteria have also been developed with reference to the criteria currently used by the Accounts Commission, the Data Protection Act 1998[2] and the Local Government (Scotland) Act 1973[3], which sets out the criteria for 'exempt items'.

14. All papers remain open to FOI requests and any exemptions are subject to the public interest test.

15. There are three main categories:
    - Statutory/ security/ legal
    - Commercial sensitivity
    - Effective conduct of business

16. The next sections offer more detail on the criteria and the relevant FOI exemptions are shown in brackets.

Statutory/ security/ legal

17. This category includes:
    - Personal information (38)
    - Danger to health and safety (39)
    - Danger to security (30)
    - Prohibitions on disclosure (26)
    - Legally privileged information (36)
    - Information provided in confidence (36)

18. We anticipate that very few Board papers would fall into this category.

[1] Freedom of Information (Scotland) Act 2002
[2] Data Protection Act 1998
[3] Local Government (Scotland) Act 1973 Schedule 7a

Personal information

19. ‘Personal information means information about any identifiable living individual. Board reports may contain information about members and others persons attending meetings (their attendance, reports of their views and opinions, actions upon them), and information about third parties who are mentioned in discussions.

20. Personal information is protected by the Data Protection Act, which makes it unlawful to transfer or release personal information unless certain conditions are met. This is recognised by section 38 of FOISA which allows personal information to be withheld if its release to a third party would contravene the Data Protection Act.

21. Some personal information dealt with by the Board could be public, and some should be private, for example if releasing it into the public domain would breach the Data Protection Act. The Information Commissioners (the bodies which regulate Freedom of Information and Data Protection[4]) have suggested that public bodies can release certain types of personal information in response to Freedom of Information requests, because doing so does not contravene the principles of the Data Protection Act and is in the interests of accountability.

22. This includes:

- Basic information about staff in a work capacity, such as names, job titles, roles and responsibilities and work contact details - much of which Audit Scotland publishes on the website.
- Grades and salary bands of staff (although not specific salaries, except for staff earning over £100,000 where the Information Commissioner suggests salaries should be disclosed).
- Decisions and actions taken by staff in an official or work capacity, unless the information is exempt for some other reason.

23. Information in these categories can be held back in rare situations where releasing it might endanger an individual's health or safety.

24. Board members serve on the Board and its committees in an official capacity. The guidance above suggests that membership on a committee, members' views and opinions expressed at meetings and actions upon them should not be withheld as personal data. This information should go into open business unless it falls under an item where another Freedom of Information exemption applies, for example a report of a committee member's opinion on a matter which is commercially sensitive.

25. Based on the Information Commissioner's guidance, the following information about third parties can be dealt with under public business and published in public minutes:

- Routine notices of the appointment, departure or promotion of staff (but not details of reasons, discussions prior to the event etc.).

[4] Data Protection is covered by the UK Information Commissioner, FOI is covered by the Scottish Information Commissioner

- Information about the roles, duties and responsibilities of staff.
- Minor references to individuals which do not convey anything substantive about them.
- Information which is already in the public domain (e.g. on the Audit Scotland website).
- Information about the decisions or actions of staff in an official or work capacity, unless it is exempt for other reasons.

26. Other personal information which might on occasion come before the Board should go into private business, as releasing it could breach the privacy rights of individuals under the Data Protection Act. The following are examples of information that should be considered in private:
    - Sensitive employment-related information about individual staff (grievance, discipline, performance etc.).
    - Information about the health, welfare or personal lives of individuals.

27. The Board will sometimes discuss posts rather than individuals. Information about a post is not necessarily personal data: e.g. discussion about creating a post will not be personal data because no one holds the post. However, information about a post will be personal information if the post can be associated with an individual through sources such as the website. Whether discussion about a post should go into public or private business will therefore depend on the wider context and the factors outlined above.

28. As personal information can make it difficult to place minutes into the public domain, it is good practice to adopt a style of writing which de-personalises minutes as far as possible.

Danger to health and safety

29. Information whose release might endanger the health or safety of any person should always be dealt with in private, as it is likely to be exempt under section 39 of FOISA. This might occur if there was a risk that placing the information in the public domain would lead to an individual receiving threats or harassment, or would aggravate a known medical condition such as a mental illness.

Danger to security

30. An item should be considered in private if it involves information whose release would be likely to endanger the organisation's security. For example, if it would:
    - reveal sensitive information about security arrangements, procedures and monitoring systems;
    - compromise IT security systems and protocols; or
    - reveal financial procedures and processes which might make it easier for someone to defraud the organisation.

31. This information is likely to be exempt under section 30c of FOISA. However, detailed information like this should not normally be recorded in minutes.

Legally privileged information

32. Discussions about legal advice provided to Audit Scotland or another organisation, or communications with the organisation's solicitors, should always be considered as private business. This information is likely to be exempt under section 36 of the FOISA.

Information supplied in confidence

33. If an agenda item involves information which then the item should be considered in private, as it may involve the discussion of information whose release would be an actionable breach of confidence (i.e. the Audit Scotland could be taken to court). Examples include information which:
    - has been supplied by an organisation or individual outside Audit Scotland
    - the information is not in the public domain; and
    - we do not have permission to make the information available; and
    - the supplier of the information has indicated that they regard it as confidential; or
    - a reasonable person would assume that permission should be sought before making the information publicly available.

34. This information is likely to be exempt from release under section 36 of FOISA.

Commercial sensitivity

35. Commercially sensitive information is information whose release would harm the commercial interests of Audit Scotland or another organisation. Items which are likely to involve commercially sensitive information should be considered as private business, as the information may be exempt under section 33 of FOISA. Examples might be:
    - Discussion about forthcoming contracts, negotiations or purchases.
    - Details of ongoing negotiations, where release of information might jeopardise the negotiations or Audit Scotland's bargaining position.
    - Sensitive pricing or operational information and trade secrets received from suppliers, tenderers, contractors etc.

36. High-level financial information about Audit Scotland's income and expenditure will not usually be commercially sensitive. However, detailed breakdowns of financial information might be exempt in certain circumstances: e.g. if it would reveal the price charged by a supplier, or the salary of an individual (see Personal data).

37. Confidential information and commercially sensitive information will often overlap. For example, information from a contractor may be supplied in confidence, and also be commercially sensitive to the contractor.

Commercial interests and the economy[5]

38. Section 33 of FOISA contains four distinct exemptions. Information may be withheld if:
    - it is a trade secret (section 33(1)(a))
    - disclosure would (or would be likely to) prejudice substantially the commercial interests of any person or organisation (section 33(1)(b))
    - disclosure would (or would be likely to) prejudice substantially the economic interests of the whole or part of the UK (section 33(2)(a)) or
    - disclosure would (or would be likely to) prejudice substantially the financial interests of an administration in the UK (section 33(2)(b)).

39. All of the exemptions in section 33 are subject to the public interest test. This means that, even if the exemption applies, the information must be disclosed unless the public interest in withholding it outweighs the public interest in disclosing the information.

40. The exemptions in section 33(1) don't last forever. In general, they can't be applied to information that is more than 15 years old. However, the exemptions in section 33(2) can be applied to information regardless of how old it is.

'Commercial confidentiality'

41. Information which is commercially sensitive is often described as being 'commercially confidential'. However, there is no single exemption in FOISA covering 'commercial confidentiality'. FOISA draws a distinction between information where disclosure would have a detrimental effect on commercial interests, and information which is 'confidential' under Scots law.

Effective conduct of business

42. This category includes papers/ information which:
    - Prejudice the free and frank provision of advice, exchange of views for deliberation or effective conduct of public affairs (30)
    - is intended for future publication (27)

Free and frank advice and discussion

43. Section 30 of FOISA allows information to be withheld if releasing it would prejudice 'the free and frank provision of advice', 'the free and frank exchange of views for the purposes of deliberation' or 'the effective conduct of public affairs'.

[5] Scottish Information Commissioner guidance
http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/section33/Section33.aspx

44. Under this criteria, it would be valid to consider in private high-level policy or strategic discussions (for example about the future of the organisation), if release of the record of the discussions would prejudice/ constrain the discussions or similar discussions in the future. However, this should be done sparingly, as Audit Scotland would need to make a strong case in order to use this exemption in response to a Freedom of Information request. It is also more likely to apply to a detailed record of who said what at a meeting, rather than to what was decided at the meeting.

Information intended for future publication

45. Section 27 of FOISA allows for information to be withheld if it is intended for future publication.

46. It would be appropriate to consider draft versions of plans and strategies in this category as these documents would be published in final form in due course.

47. The guidance on this states 'The exemption in section 27(1) applies to documents which are ready for publication and to information in draft form where further work on it needs to be carried out. It will include information published at regular intervals, such as annual or quarterly reports, or minutes of scheduled meetings, where it is easy to demonstrate a commitment to publish the information within 12 weeks. But it could also include drafts of speeches, press releases and announcements, or incomplete data from a fact-finding project, as long as the final version of the information is due to be published within 12 weeks'.

48. It would also be appropriate to consider discussion papers and options papers in this category where they are part of an ongoing process which would ultimately result in a decision paper being submitted to the Board.

FOI requirements and the public interest test

49. All of the categories and criteria should be used sparingly and the presumption should be for publication wherever possible.

50. In addition, while the FOISA exemptions have been used as a guide for helping to determine public / private papers all exemptions under the Act are subject to the public interest test.

51. The test requires authorities to undertake a balancing exercise to consider the public interest in disclosing information and the public interest in maintaining the exemption. Where the public interest in maintaining the exemption outweighs the public interest in the disclosure of the information, then the information can be withheld. If the public interest in disclosing the information is equal to or greater than the public interest in maintaining the exemption, then the information must be disclosed.

Appendix - Board dates 2016

Meeting	Submit papers	Issue papers	Meeting date
May	19/04/16	26/04/19	03/05/16
June	19/05/16	26/05/16	02/06/16
August	04/08/16	11/08/16	18/08/16
September	01/09/16	08/09/16	15/09/16
October	13/10/16	20/10/16	27/10/16
December	17/11/16	24/11/16	01/12/16