Risk Management Framework

2023-25

AUDIT SCOTLAND

Prepared by Audit Scotland
March 2023

Contents

1. Introduction

1. Audit Scotland provides the Auditor General for Scotland 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 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 is 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 doing so, 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.

7. There are five key aspects to our risk management process are illustrated in Exhibit 1.

Exhibit 1: Risk management process

Source: Audit Scotland

2. Policy statement

8. 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.

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

10. The application of risk management practices cannot and will not completely 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.

11. 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'**.

12. The importance of risk management, and the part it plays in managing the organisation, is set out in the Corporate Plan and other supporting documentation such as Business Group Plans and risk registers. It is also summarised in the Annual Report and Accounts each year.

13. 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.

14. 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.

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

16. The corporate Performance and Risk Management Group (PRMG) 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.

17. This forum is complemented by regular meetings of risk lead officers in each of the business groups, who typically meet on a two monthly basis.

18. 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.

3. Risk management approach

Risk management objectives

19. The following objectives form the basis of our Risk Management Framework. We aim to:

- 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

20. 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.

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

22. 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

23. 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.

24. 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 about risk management
- ensure that all colleagues understand our approach to, and their role in, risk management.

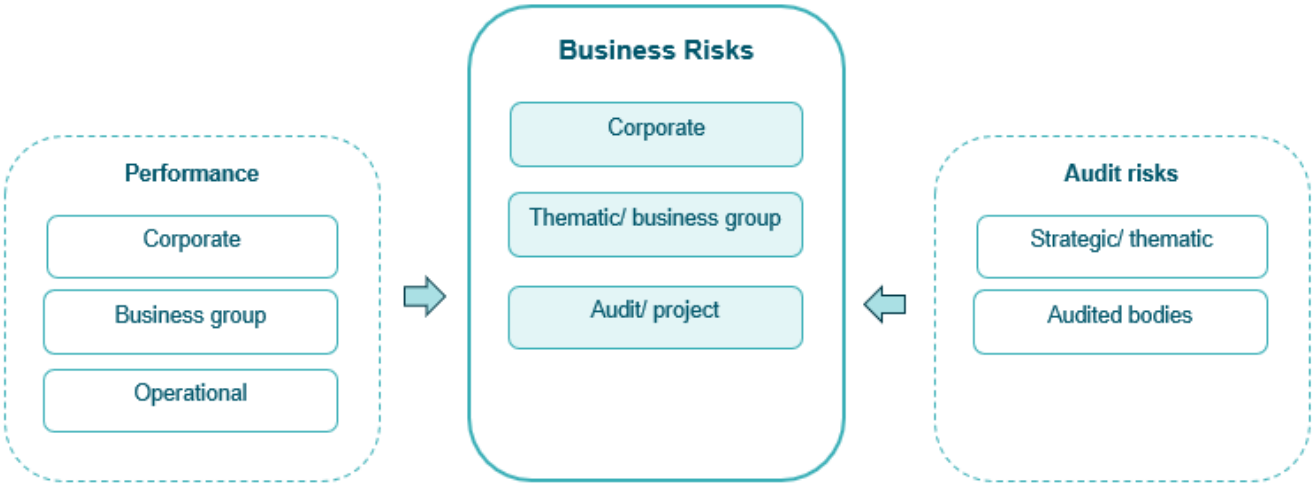
Risk management structure

25. 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 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.

26. 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.

Exhibit 2: Risk management structure



Source: Audit Scotland

27. We 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.

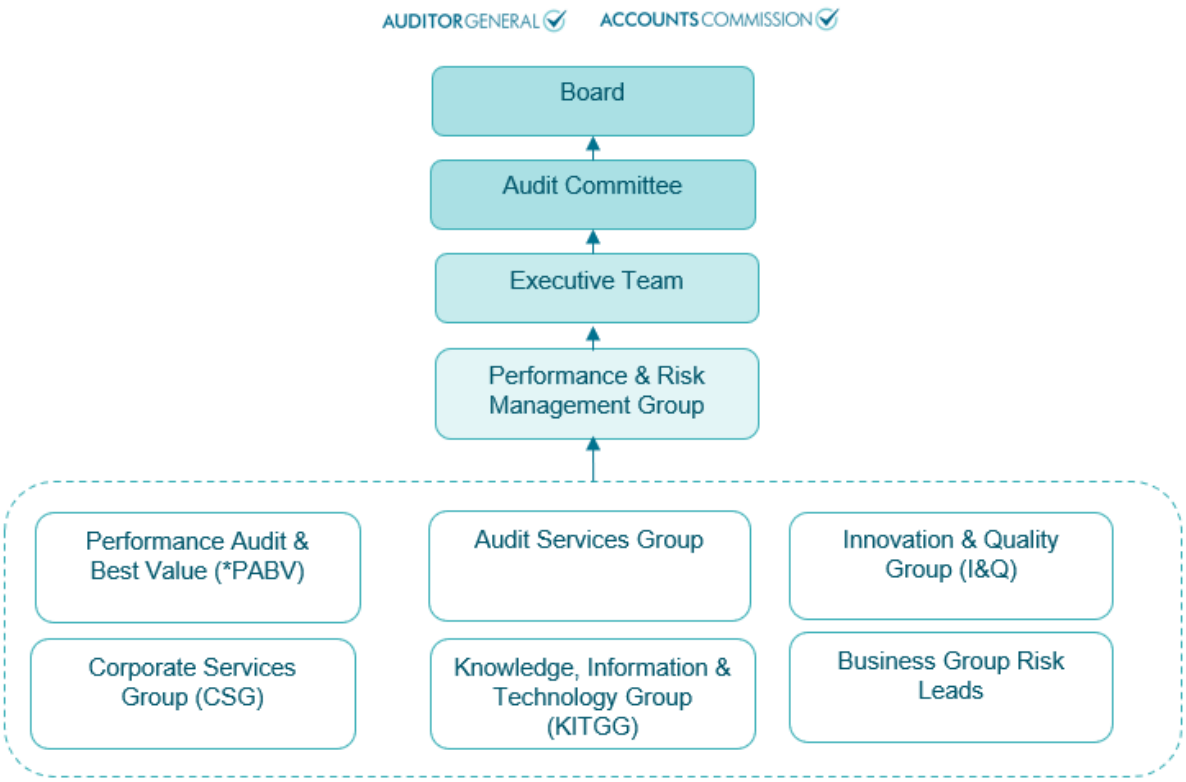
4. Risk registers

Audit Scotland's 'risk universe'

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

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

Exhibit 3: Risk universe



Source: Audit Scotland

Responsibilities

30. The Audit Scotland Board through its Audit Committee has responsibility for the risk management arrangements.

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

32. Executive 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.

33. The Audit Scotland Risk Register (ASRR) is structured around our strategic objectives, follows a standard format (Appendix 2) and includes the following elements:

- risk description
- 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.

34. Risks for action are considered by Executive Team and the Audit Committee five times a year as a minimum. Risks for monitoring, typically strategic risks - but where the risk assessment is 'green' are reported at summary level to Executive Team and the Audit Committee, and are monitored at a more detailed level by the PRMG.

35. Risk leads in each business group meet on a regular basis, typically every two months, to discuss the risk profile at the corporate ad business group level. This informs the content of the risk registers at both a strategic and operational level.

36. Other risk registers follow the same or similar format to ensure consistency across the organisation and facilitate risks being escalated, monitored and reported as appropriate, while providing a degree of flexibility in order that they are proportionate.

Risk registers

37. 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. Audit Scotland's Executive Team maintains and updates the risk register, with support from the Director of Corporate Support and the PRMG.

38. 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 is done through the PRMG. Nominated owners have responsibility for maintaining and updating risk registers in consultation with their business group leadership/ management team.

39. Audit/project Risk Registers: Separate risk registers are maintained for major audits/ projects where appropriate. 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.

5. Risk management process

Risk identification

40. 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.

41. 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)
- Audit Committee/ Executive Team risk workshops (minimum one per year)
- Executive Team/ Leadership Group strategic sessions
- monitoring of audit risks (using the audit risk management framework)
- monitoring of performance
- existing forums (board, audit committee, executive team, business group management teams, audit team/project group meetings)
- risks identified by internal/external audit.

42. It is important, therefore, that risk features as a standing agenda item on Executive Team meetings and working groups/ corporate forums across Audit Scotland where appropriate. Any risks identified should be reported for inclusion in the relevant risk register which would, in turn, be reviewed by a risk owner.

43. Additional risk prompts/tools are included as appendix 3 to assist with this.

Risk analysis and assessment

44. Once a risk is identified the risk is assessed. Risks are assessed considering – likelihood of the risk occurring, and if that risk was to occur, what the impact (i.e. consequences) on the organisation would be.

45. Likelihood is 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

Source: Audit Scotland

46. 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

47. 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.

48. 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).

49. 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 and/ or an ongoing basis and with ongoing active monitoring. 'Red risks' at Business Group level should be included in the Audit Scotland risk register.
Medium	11 - 19	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.

Source: Audit Scotland

Risk response

50. 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 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 mitigating actions then it can probably be tolerated.

Risk mitigation

51. These are the controls and actions put in place to reduce the likelihood of 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.

52. 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.

53. 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

54. 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.

55. It is vital 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.

56. 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 be 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.

57. 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

58. 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.

6. Monitoring and reporting arrangements

Monitoring risks

59. 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.

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

61. The Director of Corporate Support, and the PRMG review risk on a quarterly basis. This includes a review of the high risks facing Audit Scotland and mitigating action plans. The Director of Corporate Support links directly with the Executive Team and will advise them on which risks to escalate/ de-escalate for inclusion or deletion from the Audit Scotland risk register.

62. The PRMG also reviews the 'risk for monitoring'. These are strategic risks which are important, but which are within risk tolerances ('green risks') and escalates these to Executive Team where required.

63. Where any significant risks emerge which require attention and action outwith the normal risk monitoring and reporting cycle these can be escalated immediately to the most appropriate forum.

Action planning

64. In situations where a risk is classified as 'to be treated', and scores either 'amber' or 'red' then action must be taken. This includes consideration of:

- the risk owner reviewing the actions to be taken
- the controls that need to be put in place / strengthened
- the action owner, and

- the timescale for implementation.

65. Additionally, the action plan should indicate whether planned actions are aimed at reducing the likelihood and/or the impact of the risk. The PRMG update the Audit Scotland risk register for Executive Team to consider and approve, including any additional actions required to further reduce risks.

Reporting and assurance arrangements

66. Audit Scotland's risk management framework is 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.

67. The arrangements, include:

Corporate level

68. The Audit Scotland's Board reviews and approves risk management policies and strategies. It will take advice from the Audit Committee on these matters.

69. 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 actions planned 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.

70. The Audit Committee reviews the Audit Scotland Risk Register at each meeting and receives an annual statement on risk management from the internal auditors. The committee also considers input from other sources of assurance as appropriate.

71. The Audit Committee can considers a detailed risk ‘deep dive’ on one or more of the identified risks at its meetings. These ‘deep dives’ can take a variety of forms, depending on the nature of the risk and how best this can be examined. This may include the consideration of risk interrogation reports, detailed subject specific reports, presentations and workshops. The Audit Committee approves the schedule of risk deep dives each year, though this can be varied to accommodate new or emerging risks where this is required.

72. The Executive Team maintains, reviews and updates the Audit Scotland Risk Register on the key risks facing the organisation on a regular basis. The Executive Team while retaining ultimate responsibility for updating the Audit Scotland risk register delegates the detailed review work to the Director of Corporate Support and the PRMG.

Business Group level

73. Each Executive Director/Head of a Business Group reviews risks and actions in mitigation of risk on a regular basis as an integral part of the business planning process. These officers 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.

74. Risk owners 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 owners 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.

75. The Director of Corporate Support and PRMG, after considering feedback from risk owners, updates the Audit Scotland risk register and provide the Executive Team with an overview of the risk profile across Audit Scotland.

Audit/project level

76. Risks associated with audits/projects will be reviewed by the manager/project sponsor or officer responsible for maintaining, where appropriate, a project risk register based on delegated authority.

77. 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

78. 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.

79. The risk maturity model will be reviewed periodically by internal audit with findings discussed by the Executive Team (via the PRMG). The Executive Team 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 where appropriate.

Appendices

Appendix 1: Responsibilities

Level	Role & responsibilities	Frequency
Audit Scotland Board	• Setting the tone at the top for risk management throughout the organisation. • 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	• Approving the overall risk management arrangements including the appetite for risk. • 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 Quarterly Quarterly
Accountable officer	• Specific personal responsibility for signing the annual accounts including the Accountable Officer's Governance Statement.	Annually
Audit Scotland Executive Team	• 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 Executive Team or Leadership Group.	Quarterly As required

Level	Role & responsibilities	Frequency
	• Approving and recommending to Audit Committee draft risk policies and 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	• 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 owners to co-ordinate risk management activity within their areas of responsibility.	Ongoing
Director of Corporate Support and Performance and Risk Management Group (PRMG)	• Support Executive Team and Audit Committee in the management of risk. • 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, risks where controls are not effective. • Reviewing the 'risk for monitoring' risks and escalating these where required.	Quarterly Ongoing

Level	Role & responsibilities	Frequency
	• Challenging progress against risk action plans holding those to account for agreed actions. • Liaising with risk owners to identify possible corporate risks. • Advising Executive Team 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 owners.	
Knowledge, Information and Technology Group (KITGG)	• Risk owners for information and technology risks. • Owners of the Information Risk Register. • Reviewing information and technology risks at each two monthly KITGG meeting. • Formulating risk responses as appropriate. • Nominating and appointing risk owners to co-ordinate risk management activity within their areas of responsibility (typically Information Asset Owners). • Advising Executive Team on risks to be escalated for inclusion in the Audit Scotland risk register.	Every two months
Risk owners (Senior staff nominated by their Director to support and be integral to the risk management framework) (Includes Corporate Services Group Managers who cover cross cutting risks).	• Supporting Audit Scotland's risk management framework. • 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 colleagues to ensure that risk registers are kept up to date. • Escalating risks where appropriate. • Being a key reference point for staff in providing support and advice on risk management. • Maintaining and updating business group risk registers.	Ongoing

Level	Role & responsibilities	Frequency
	• Working with other risk owners to ensure consistency of approach across the organisation. • Challenging other 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.	
Business Group Risk Leads	• Maintaining and updating business group risk registers • Regular liaison with other rsk leads to inform the update of business group and corporate risk registers	
Working groups	• Ensuring that risks is appropriately considered at meetings and minuted where appropriate. • Facilitate the sharing of best practice and lessons learnt.	Per timetabled meetings
Colleagues	• Following Audit Scotland's risk management framework. • Understanding risk and being aware of the role of risk owners. • 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 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

Risks for action/ attention

No	Risk description	Gross risk			Controls in place	Net risk			Prev. net risk and	Planned actions, owners and timescales	Target Risk	Owner
		L	I	Tot	(Preventative/*remedial*)	L	I	Tot	change		(Date)	
A1	Failure to protect **digital infrastructure,** systems and information Failure to **recover** to business as usual after a successful cyber attack (Strategic risk: BWCO)	5	5	25	**Active controls** • Digital Services Strategy 2021+ • Digital policies & procedures. • Network system defences. • Service diversification. • Training & education. • Data preservation, archiving & retention. • Secure authentication & permissions. • Management preparedness. (24/7) • Network monitoring. • Vulnerability patching. • Digital security skills & capacity. • IAR: Digital Strategy 2022/23 (W&B) **Monitoring controls** • ISO27001 certification. • Digital security standing item for KITGG/ ET/Audit Committee. • Monthly security update to CISO(COO). • System recovery tests • External scrutiny (including ISO, Internal Audit etc). • Information Risk Register.	4	5	20	20 ⇨	**Actions** • Investment in additional h/w & s/w re digital security and resilience. • £60k committed to secure MKI data & £227k annual cloud services contract renewed to protect all non MKI data • Implementation of Digital Services Strategy to further strengthen security. • Objective 1: *Enhance our Cyber Security* – 'We will continue to improve the safety of our online and remote work environments, ensuring cyber security is a priority and embedded in everything we do.' • Maintain ISO 27001 certification. **Review** • Ongoing by DSMT, KITGG and MT, 6 monthly reports to Audit Committee. • ISO 27001 re-certification audits	15 Ongoing	DR

Notes

- 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.
- Risks are categorised as strategic or operational, operational risks with a high net risk score are included in the corporate risk register
- Risk register reports to Executive Team and the Audit Committee group risks under our strategic objectives (Delivering World Class Audit, Being a World Class Organisation.
- Gross and net risk scores are 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
- Controls are set out and categorised as either active, responsive or monitoring controls
- Net risk from the previous review period are included in the register for monitoring purposes and are accompanied by a direction of travel indicator
- The change in risk profile from one period are explained in the register or covering report
- Actions indicate what further steps are being taken to manage the risk, the objectives of these actions, review points
- Target risk is the level of tolerable risk where no further mitigating actions are required and where actions will have managed the risk to an acceptable level by a date or timeframe
- Risk registers should follow the same format as the Audit Scotland risk register unless there is a clear reason not to

Appendix 2: 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 Director of Corporate Support/ PMRG will develop and provide 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

Strategic priorities prompts

Is there a risk to/of…

Delivering World Class Audit
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
Failure of legitimacy - Our vision is not shared by key stakeholders
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 process - Our audit work is not carried out in accordance with procedures
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 to influence development of the scrutiny framework for new financial powers and fiscal framework.
Failure of communication (external) - Our messages are not clear to stakeholders (inc audit reports and other corporate communications)
Being a World Class Organisation
Failure of vision - We do not have a clear vision for the organisation
Failure to provide the services required by the Auditor General and/ or the Accounts Commission
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 to support our people - we fail to provide the support, training, resources to colleagues in order that they can operate effectively
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 capacity - We are unable to meet the demand for audit under the new financial powers and fiscal framework and changing constitutional arrangements
Failure of resourcing (financial) - Budget planning, Budget management, Procurement, Payment
Failure of resourcing (assets) - Edinburgh office move, office availability
Failure of resourcing (digital) - 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 and 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 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 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 and managers are trained in risk management techniques. Risk management is written into performance expectations of	There are clear links between objectives and risks at all levels. Risk information is documented in a risk register. The organisation's risk appetite is used in the scoring system for	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 organisation have been	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 basis (annually). Directors require interim updates	The organisation's risk management approach and the Board's risk appetite are regularly reviewed and refined in light of new risk information reported. Management assurance is provided

	Risk Governance	Risk identification & assessment	Risk mitigation & treatment	Risk reporting & review	Continuous improvement
	managers. Management and executive level of responsibilities for key risks have been allocated.	assessing risks. All significant projects are routinely assessed for risk.	selected and implemented.	from delegated managers on individual risks which they have personal responsibility.	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 most appropriate responses to 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 information is brought together for some parts	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 to 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 board.	The Board gets minimal assurance on the effectiveness of risk management.

	Risk Governance	Risk identification & assessment	Risk mitigation & treatment	Risk reporting & review	Continuous improvement
	management of identified risks. Management and executive level of responsibilities for key risks have been allocated.	of the organisation. Most projects are assessed for risk.			
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.
Naive	No formal approach developed for risk management. No	Processes for identifying and evaluating risks and responses are not	Responses to the risks have not been designed or implemented.	There are no monitoring processes or regular	Management does not assure the Board on

	Risk Governance	Risk identification & assessment	Risk mitigation & treatment	Risk reporting & review	Continuous improvement
	formal consideration of risks to business objectives, or clear ownership, accountability and responsibility for the management of key risks.	defined. Risks have not been identified nor collated. There is no consistent scoring system for assessing risks.		reviews of risk management.	the effectiveness of risk management.

Audit Scotland Risk Management Framework

2023-25

Audit Scotland's published material is available for download on the website in a number of formats. For information on our accessibility principles, please visit:
www.audit-scotland.gov.uk/accessibility

For the latest news follow us on social media or
subscribe to our email alerts.

Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN
Phone: 0131 625 1500 Email: **info@audit-scotland.gov.uk**
www.audit-scotland.gov.uk

AS.4.0