Audit and Assurance Committee Handbook

August 2026

Scottish Government
Riaghaltas na h-Alba

Contents

Foreword 3

Glossary of Terms 6

Chapter 1: Good Practice Principles for Audit and Assurance Committees 7

Chapter 2: Membership, Independence, Objectivity and Understanding 8

Chapter 3: Skills 11

Chapter 4: Role and Scope 12

Chapter 5: Communication and Reporting 24

Annex A: The role of the Chair: good practice 26

Annex B: Committee support: good practice 29

Annex C: Model letter of appointment 31

Annex D: Model terms of reference 34

Annex E: Example Annual Core Work Programme 39

Annex F: Governing the internal audit function 40

Annex G: Key Questions for and Audit and Assurance Committee to Ask 43

Annex H: Competency framework 49

Annex I: Risk Control Framework 50

Annex J: Self-assessment checklist 52

Foreword

At its simplest, corporate governance helps make sure an organisation is achieving its objectives in the best way it can. The scale, variety and nature of risks which the public sector is navigating, including fiscal challenges, cyber threats, digital disruption and geopolitical uncertainty, demands robust and effective governance. In this context, the role of the Audit and Assurance Committee* is more important than ever.

The role is a challenging one. It needs independent and objective members with an appropriate range of skills and experience. Audit and Assurance Committees must provide insight and effective, constructive challenge.

Since the Handbook** was last reviewed in 2023, the Global Internal Audit Standards (GIAS) have come into effect, replacing the Public Sector Internal Audit Standards. The GIAS, as they apply to internal audit functions in the public sector in the UK, introduced mandatory requirements for Audit and Assurance Committees in relation to their role in enabling an effective internal audit function.

This revision of the Handbook sets out to support Audit and Assurance Committee effectiveness by clarifying the fundamental principles relating to the role, membership and work of Audit and Assurance Committees in those organisations to which the Scottish Public Finance Manual (SPFM) is directly applicable. It can also be used as a good practice guide for organisations in which the SPFM is not directly applicable.

A degree of flexibility, pragmatism and proportionality will be needed in applying the guidance in this Handbook to individual organisations. For example, the use of the term “Board” referred to in chapter four should be interpreted in the context of the “On Board” Guidance (January 2023), which defines the differences between Statutory and Management Advisory Boards. Subject to these caveats, any

significant non-compliance with the principles in this Handbook should be explained and reported in the annual Governance Statement.

The Handbook emphasises the sources of assurance available to Audit and Assurance Committees in addition to internal and external audit. We encourage all organisations within the Scottish Government family to define their assurance needs, map their various sources of assurance and develop an integrated approach to assurance which will secure best value for the public purse and embed best practice principles within their organisation.

We commend this Handbook to you.

Joe Griffin	Jennifer Inglis-Jones
Permanent Secretary	Director of Internal Audit and Assurance

* Alternatively referred to as the Audit Committee / Audit and Risk Committee / Audit and Risk Assurance Committee. For the purposes of this Handbook - the term Audit and Assurance Committee will be used in a generic context.

**The *Scottish Government Audit and Assurance Committee Handbook* draws on, and is consistent with, generally accepted principles concerning corporate governance and the role of audit and assurance committees. Relevant source publications include:

- HM Treasury: Audit and Risk Assurance Committee Handbook (April 2025)
- GIAS (January 2024 – effective from 2025)
- HM Treasury: Corporate Governance in Departments: Code of Good Practice (April 2017)

- The Good Governance Standard for Public Services

- Financial Reporting Council: The UK Corporate Governance Code (January 2024)
- Scottish Public Finance Manual (March 2026)
- On Board: A Guide for Members of Statutory Boards in Scotland (January 2023)
- On Board: A Guide for Members of Management Advisory Boards (March 2017)

Glossary of Terms

AO - Accountable Officer

DG - Director General

DIAA - Directorate of Internal Audit and Assurance

GIAS - Global Internal Audit Standards

NDPB - Non-Departmental Public Body

NXD - Non-Executive Director

SG - Scottish Government

SGAAC - Scottish Government Audit and Assurance Committee

3LM - Three Lines Model (previously, Three Lines of Defence)

Chapter 1: Good Practice Principles for Audit and Assurance Committees

Principle 1: Membership, independence, objectivity and understanding

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

Principle 2: Skills

The committee should collectively own an appropriate skills mix to allow it to carry out its overall function.

Principle 3: Role and Scope

The committee should support the Accountable Officer (AO) and Board by reviewing the comprehensiveness and reliability of assurances on governance, risk management, the control environment and the integrity of financial statements and the annual report.

The scope of the committee's work should be defined in its terms of reference and should encompass all the assurance needs of the AO and Board. This should include providing insight, scrutiny and challenge to management. Within this, the committee should have particular engagement with the work of Internal Audit, risk management, the External Auditor, and financial management and reporting issues.

Principle 4: Communication and Reporting

The committee should ensure that it has effective communication with all key stakeholders, for example, the Board, the Head of Internal Audit, the External Auditor and other relevant assurance providers e.g. second line governance, risk and assurance functions. In addition, the role of the Chair of the committee and

provision of appropriate secretariat support are important elements in achieving committee effectiveness. Good practice guidance on these roles is provided, respectively, in **Annex A** and **Annex B**.

Chapter 2: Membership, Independence, Objectivity and Understanding

Independence

2.1 An effective Audit and Assurance Committee must have members who are both independent and objective. The AO and Board should be supported by an Audit and Assurance Committee with no executive responsibilities, comprising of at least three members. The Chair should be a Non-Executive Member (NEBM) [sometimes called a Non-Executive Director (NXD)] with relevant experience. There should be at least one other NEBM/NXD on the committee; when there are insufficient NEBMs/NXDs to form the committee, independent external members must be appointed (but to retain independence, the chair of the board should not be a member of the committee). The committee may also need to seek further independent, non-executive membership from sources other than the Board in order to ensure an appropriate level of skills and experience. These members are appointed to the Audit and Assurance Committee but not to the Board and the independence of the committee from an executive function should be its guiding ethos. In order to operate in an independent and competent manner, the committee should possess the requisite knowledge and skills to effectively engage with and challenge the organisation (see Chapter 4: Role and Scope).

Relationship with the Executive of the organisation

2.2 Executive members of the organisation should not be appointed to the Audit and Assurance Committee. The role of the members of the executive is to attend, to provide information, and to participate in discussions, either for the whole duration of a meeting or for particular items.

2.3 The AO and the Finance Director should routinely attend the Audit and Assurance Committee. It is also normal for the Head of Internal Audit and a representative of the External Auditor to attend. The terms of reference, which form the basis of the relationship between the body and internal audit, should also provide for the Audit and Assurance Committee to sit privately without any non-members present for all or part of a meeting if they so wish.

2.4 It is also good practice for the Chair of the Audit and Assurance Committee to meet the AO, the Finance Director, the Head of Internal Audit and the External Auditor's senior representative outside of the formal committee structure (see Chapter 5: Communication and Reporting).

Other participants

2.5 It is common for representatives of sponsoring or sponsored bodies to attend Audit and Assurance Committee meetings (for example, a member of the core Scottish Government may attend the Audit and Assurance Committee of one of its Executive Agencies or bodies). However, such representatives should not be appointed as members of the committee.

Conflicts of interest

2.6 The process for recording declarations of interest, including conflicts, in the Audit and Assurance Committee should mirror the processes used at Board level. Each member of the committee should take personal responsibility to declare proactively any potential conflict of interest arising out of business on the committee's agenda or from changes in the member's personal circumstances. The Chair should then determine an appropriate course of action with the member. For example, the member might simply be asked to leave while a particular item of business is taken. Where the conflict would prevent the member of the committee from discharging their role, they may be asked to stand down from the committee. If it is the Chair who has a conflict of interest, the Board or AO should ask another

member of the committee to lead in determining the appropriate course of action. A key factor in determining the course of action will be the likely duration of the conflict of interest: a conflict likely to endure for a long time is more likely to suggest that the member should leave.

Terms of appointment

2.7 All members of the Audit and Assurance Committee should have a clear understanding of:

- what is expected of them in their role, including time commitments
- how their individual performance will be appraised, including a clear understanding of what would be regarded as unsatisfactory performance and the criteria which would indicate the termination of Audit and Assurance Committee membership should be considered
- the duration of their appointment, a maximum of six years (fixed for three years with an opportunity to renew for three years)
- training required and how this will be provided

2.8 The terms of appointment of an Audit and Assurance Committee member should be clearly set out at the time of appointment. A model letter of appointment is set out at **Annex C**. The letter should also specify what other activities the individual may or may not undertake in relation to the organisation. The impact on independence of any remuneration from other activities should be given careful consideration.

Chapter 3: Skills

The committee should collectively own an appropriate skills mix to allow it to carry out its overall function. Range of skills

3.1 The committee is charged with supporting the Board and AO of the organisation gain the assurance they need on risk management, governance and internal control. So, it needs a range of skills and experience relevant to various aspects of risk, governance and control. A competency framework for an Audit and Assurance Committee is at **Annex G**.

3.2 At least one member of the committee should have recent and relevant financial experience. This experience should be sufficient to allow them to engage competently with financial management and reporting in the organisation, and associated assurances.

3.3 The committee should identify, and agree with the Board and AO, the other skills required for committee effectiveness. These identified skills should inform the appointment of members of the committee. The required skillset should be periodically reviewed.

3.4 Although Audit and Assurance Committee members are recruited for their individual skills, it is vital that they are able to work collaboratively and collectively hold the requisite skills and experience to discharge their role.

Additional skills

3.5 The committee should be empowered to either:

- co-opt members for a period of time (not exceeding a year, and with the approval of the Board and/or AO) to provide specialist skills, knowledge and experience that the committee needs at a particular time; (Co-opted members may be

remunerated at an appropriate rate for the time and effort they are expected to contribute)

- procure specialist advice at the expense of the organisation on an ad-hoc basis in order to support particular committee business. Budgets for such procurement should be approved by the Board and/or AO

Training and development

3.6 All committee members, whatever their status or background, will have training and development needs. Those who have recently joined the Audit and Assurance Committee will need induction training, either to help them understand their role; or if they have Audit and Assurance Committee experience elsewhere, to help them understand the organisation. In particular, those joining a public sector Audit and Assurance Committee for the first time will need training to help them understand public sector standards, especially those relating to governance and accountability and internal audit.

3.7 The Chair should, in addition, ensure that all committee members have an appropriate programme of engagement with the organisation and its activities to help them understand the organisation, its objectives, business needs, priorities and risk profile. Consideration should be given to underpinning such programmes with training and/or learning plans.

Chapter 4: Role and Scope

Supporting the Board and AO

4.1 AOs and Boards have many issues competing for their attention. One of the challenges they face is knowing whether they are giving their attention to the right issues. Key to addressing this, is assurance, defined as: “an evaluated opinion,

based on evidence gained from review, on the organisation's governance, risk management and internal control framework."

4.2 Assurance draws attention to the aspects of risk management, governance and control that are functioning effectively and the aspects which need to be given attention to improve them. An effective risk management framework and a risk-based approach to assurance helps an AO and Board to judge whether or not its agenda is focussing on the issues that are most significant to achieving the organisation's objectives and whether best use of resources is being made. The Audit and Assurance Committee can help the AO and Board to formulate their assurance needs and consider how well assurance provided meets these needs by gauging the extent to which assurance on risk management is comprehensive and reliable. Assurance cannot be absolute, so the committee will need to know that the organisation is making effective use of the finite assurance mechanisms at its disposal, targeting areas of greatest risk. This can include carrying out a "Deep Dive" exercise of risks that the committee determines are key threats to the organisation.

4.3 Formulation of the specific assurance need is key to determining the resource that needs to be dedicated to delivery of assurance in the organisation. Key elements include:

- the strategic outcomes and objectives which the organisation is charged to deliver, and the associated risks and control mechanisms
- the external environment in which the organisation operates and the risks to the delivery of its strategic outcomes and objectives
- the sources of assurance available
- the level of confidence required in assurances, including the extent to which the range of assurance providers can be relied on by Internal Audit in delivering its overall opinion on risk, control and governance in accordance with the GIAS

4.4 A well-designed assurance framework will help. At its simplest, this will identify all the key sources of assurance in the organisation and seeks to orchestrate them to best effect. This can help to ensure that gaps are reduced or eliminated, and unnecessary duplication avoided. A conceptual model that is often used to help to categorise the various sources of assurance is the “three lines of defence”, referenced in the HM Treasury document, “Role and Scope of the Committee, section 5.5&5.6 (Aug 2025), and the Orange Book, Annex 2(May 2023). The Global Institute of Internal Auditors produced an update paper, “Three Lines Model” in January 2021 and the Scottish Government DIAA interpreted it for the core Scottish Government and public bodies in the below diagram, further detail of the work of Internal Audit is provided later in the chapter.

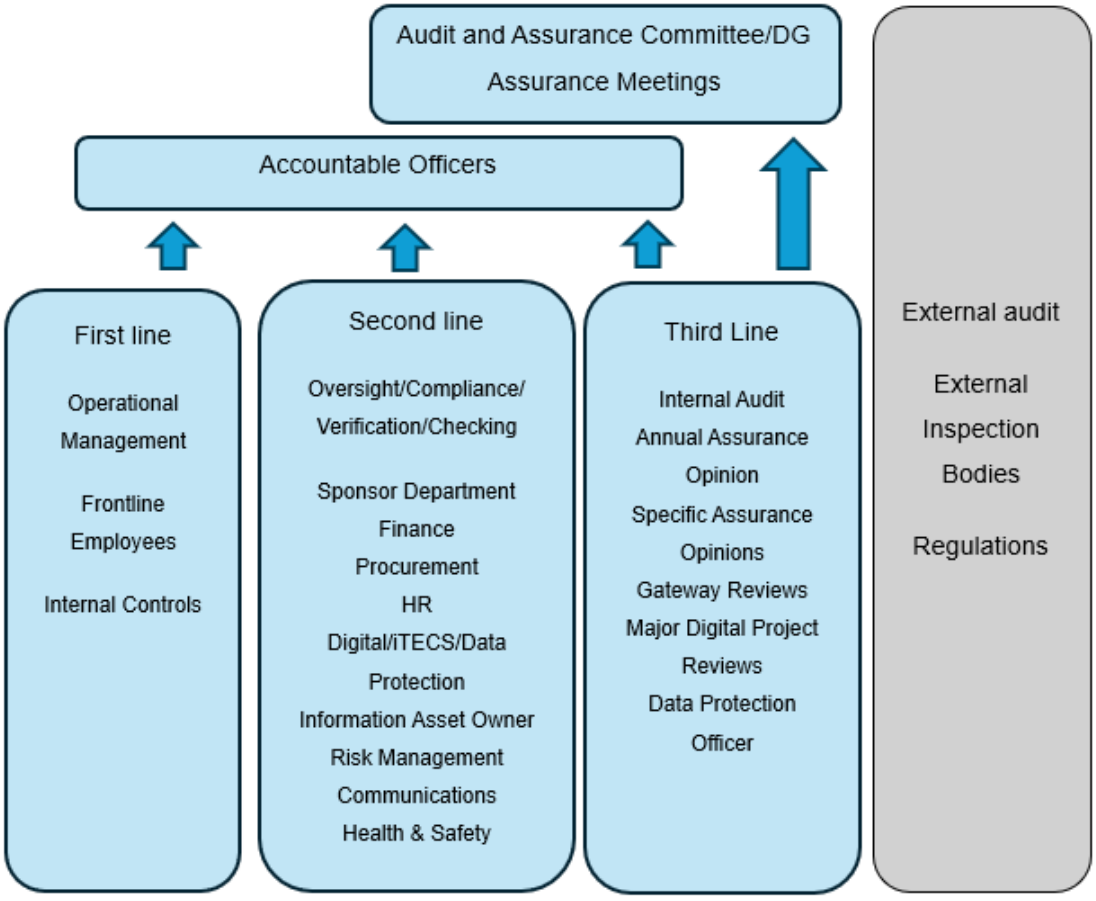

Figure 1: Scottish Government DIAA “three lines of defence”

Figure description:
Lines 1-3 all feed information and insights to their Accountable Officers. Accountable Officers and the third line (independent assurance) feed information and insights to Audit and Assurance Committees and DG Assurance Meetings.
First line: Operational Management, Frontline Employees and Internal Controls.
Second line: Oversight/Compliance/Verification/Checking by Sponsor Department or other functions like Finance, Procurement, HR, Digital, iTECs or Data Protection, Information Asset Owner, Risk Management, Communications, Health & Safety.
Third Line: Independent assurance from Internal Audit, Annual Assurance Opinion, Specific Assurance Opinions, Gateway Reviews, Major Digital Project Reviews, or Data Protection Officer.
Outwith the internal lines of defence sits external audit, external inspection bodies and regulations.

4.5 An understanding of the three lines of assurance can help the Audit and

Assurance Committee to play a key role in helping the AO and Board establish an optimum mix of assurance. For example, management and oversight assurance activities can be harnessed to provide coverage of routine operations, with Internal Audit activity more effectively targeted at riskier and/or more complex areas. As well as strengthening assurance arrangements, this helps the Audit and Assurance Committee to demonstrate added value to the organisation.

4.6 The overall provision of assurances to the AO and Board should be reviewed by the Audit and Assurance Committee, which should constructively challenge:

- whether the nature and scope of the assurance providers' activity meets the AO's and Board's assurance needs
- the credibility and independence of each provider

- where appropriate, the actual assurances to test that sufficient reliable evidence and that conclusions are reasonable in the context of the evidence

The committee should also be proactive in commissioning assurance work from appropriate sources if it identifies any significant risk, governance and control issues which are not being subjected to sufficient review, and in seeking assurance on weaknesses identified by reviews are actually remedied by management.

A list of “prompt” questions for Audit and Risk Assurance Committees to ask is provided at **Annex F**.

4.7 The committee’s view of the overall assurance landscape may draw attention to areas where:

- risk is being appropriately managed (no action needed)
- risk is inadequately controlled (action needed to improve control)
- risk is over controlled (resource being wasted which could be diverted to other use)
- there is lack of evidence to support a conclusion on how risks are being identified and managed. If this concerns areas material to the organisation’s operations, more assurance work may be needed, subject to an assessment of costs and benefits

  All of the above should be considered in line with the agreed risk appetite, (Orange Book, supplementary Guide “Risk Appetite Guidance Note”, (May 2023). Guidance is also found in the SG Risk Management Stage Two: Assessing Risk and Risk Appetite, the SG Risk Appetite Statement Pack

4.8 Assurance should be obtained on the management of risks, and the delivery of organisational objectives. The governance structure of the departmental family/group will therefore need to ensure that there is effective communication on risks and control to ensure appropriate visibility of and timely action on such matters as well as to feed into the annual Governance Statement.

4.9 Similarly, assurance on the risk and control environment should also encompass services outsourced to external providers, including shared service arrangements, so that all key elements of the organisation are considered as parts of the wider organisation and business function.

4.10 It is also good practice to have reasonable oversight of risks that cross organisational boundaries, for example, in major projects. This could include a Chairs of Audit and Assurance Committee Forum. Any such forum should focus on assurances on cross organisational governance, risk and control arrangements.

Internal and external audit

4.11 For any government organisation there will always be two significant sources of independent and objective assurance: Internal Audit and External Audit.

4.12 The purpose of Internal Audit is intended to assist internal auditors and internal audit stakeholders (AO and Board/Executive of the organisation) in understanding and articulating the value of Internal Audit. GIAS: Domain 1 (April 2024).

4.13 The purpose of External Audit, working to the Auditor General and under the Public Finance and Accountability (Scotland) Act 2020, audit the accounts of most public bodies in Scotland, except local government sector, and report on their financial health and performance, Audit Scotland, Code of Audit Practice, (2021)

4.14 These are likely to be some of the most significant sources of assurance drawn upon by the committee in discharging its responsibilities. This is because the Head of Internal Audit has, in accordance with the GIAS Application Note (December 2024), a responsibility to provide an annual opinion on the overall adequacy and effectiveness of the organisation's governance, risk management and control processes. There is consequently a major synergy between the purpose of the Head of Internal Audit and the role of the Audit and Assurance Committee.

4.15 From 1 April 2025 the requirements of this Application Note and of the Global Internal Audit Standards apply to work on internal audit engagements commenced on or after this date, GIAS Application Note (December 2024). GIAS have been, issued by a conglomerate of bodies including CIPFA and in collaboration with the Chartered Institute of Internal Auditors (Chartered IIA). GIAS became the mandated framework for internal audit practice across the UK public sector. These standards and Topical Requirements, are supplemented by the GIAS in the UK Public Sector Application Note, which provides UK-specific interpretations and additional requirements to ensure the standards are appropriately contextualised for the public sector environment. Within the Scottish Government shared service model, the Scottish Government Audit and Assurance Committee (SGAAC) is designated as the overriding committee responsible for the governance and implementation of Domain III of GIAS, which relates to the governance of the internal audit function. The requirements of Domain III will be fulfilled through SGAAC and reported annually to the relevant Audit and Assurance Committees that fall under the shared service arrangement.

4.16 The role of the Audit and Assurance Committee in relation to Internal Audit should include advising the AO and Board on:

- the Internal Audit strategy and periodic Internal Audit plans, forming a view on how well they reflect the organisation's risk exposure and support the Head of Internal Audit's responsibility to provide an annual opinion
- the adequacy of the resources available to Internal Audit
- the Internal Audit charter/terms of reference for Internal Audit
- the results of Internal Audit work, including reports on the effectiveness of systems for governance, risk management and control, and management responses to issues raised
- the annual Internal Audit opinion and annual report

4.17 In the Scottish Government context, the Auditor General for Scotland is responsible for appointing the external audit of most public sector bodies in Scotland and reporting on their financial health and performance. External Audit work is carried out by Audit Scotland staff and appointed auditors, including private firms. This includes the audits of financial statements as well as performance and Best Value audits. All external auditors appointed by the Auditor General are required to follow the Code of Audit Practice which outlines their responsibilities. Once appointed, auditors act independently in carrying out their responsibilities and in exercising professional judgement.

4.18 External auditor responsibilities are derived from statute, the Code of Audit Practice, International Standards on Auditing (UK and Ireland) and professional requirements.
These include:

- audit of financial statements and related matters: appointed auditors are required to give an opinion on the financial statements as to: whether they give a true and fair view of the financial position of audited bodies and their expenditure and income; whether they have been properly prepared in accordance with relevant legislation, the applicable accounting framework and other reporting requirements; the regularity of the expenditure and income (not required for local government)
- wider scope audit: the Public Finance and Accountability (Scotland) Act 2000 gives the Auditor General the right to initiate examinations into the economy, efficiency and effectiveness with which audited bodies and certain other bodies have used their resources to discharge their functions. The results of such examinations (known as Section 22 and Section 23 Reports) may be presented to the Scottish Parliament and considered by its Public Audit Committee. Appointed auditors are responsible for notifying the Auditor General when circumstances indicate that such a statutory report may be required

4.19 External auditors will report annually to those charged with governance on the results of their work covering both the financial statements and wider scope audit work. Audited annual financial statements including the independent auditors' reports, and reports by the Auditor General are sent to Scottish ministers to be laid before the Scottish Parliament.

4.20 It is important that the Audit and Assurance Committee engages regularly with external audit. The committee should consider the results of external audit work and the proposed actions against audit recommendations. The committee should also consider planned external audit activity and enquire about the level of co-ordination and engagement between internal and external audit to ensure there is no unnecessary duplication of audit work.

Governance

4.21 It is essential that the committee understands how governance arrangements support achievement of the organisation's strategies and objectives, especially:

- the organisation's vision and purpose
- mechanisms to ensure effective organisational accountability, performance and risk management
- role definitions, committee and other structures to support effective discharge of responsibilities, decision making and reporting
- the development, operation and monitoring of the system of internal controls and whether these will provide timely warnings of any failings
- promotion of appropriate ethics and values within the organisation
- communication of management information, including on risk and control among the board and to appropriate areas of the organisation
- relations with arm's length bodies, including reporting functions to relevant Audit and Assurance Committees and Scottish Government

Risk management and the control environment

4.22 It is also essential that the committee:

- understands the organisation's business strategy, operating environment and the associated risks, taking into account all key elements of the organisation as parts of an "Extended Enterprise"
- understands, where applicable, the role and activities of the Board (or equivalent senior governance/advisory body) in relation to managing risk
- discusses with the Board its policies, attitude to and appetite for risk to ensure these are appropriately defined and communicated so management operates within these parameters
- understands the framework for risk assessment, management and assurance and the assignment of responsibilities
- critically challenges and reviews the risk management and assurance framework providing assurance that the arrangements are actively working in the organisations, whilst ensuring that the management of risk remains the responsibility of the Executive/AO
- critically challenges and reviews the adequacy and effectiveness of control processes in responding to risks within the organisation's governance, operations, compliance and information systems
- considers whether the risk management system will be effective in identifying new and emerging risks

Financial management and reporting

4.23 The committee should consider significant accounting policies, any changes to them and any significant estimates and judgements, if possible before the start of the financial year. It should also review the clarity and completeness of disclosures in the year-end financial statements and consider whether the disclosures made are set properly in context.

4.24 The committee will not itself be able to review the accounts in detail in order to advise the AO whether they are true and fair. The committee should expect a comprehensive overview of the financial statements by the Finance Director (or equivalent role), including comparisons with the prior year and current year budget, and an explanation for any issues arising. In reaching a view on the accounts, the committee should consider:

- key accounting policies and disclosures
- assurances about the financial systems which provide the figures for the accounts
- the quality of the control arrangements over the preparation of the accounts
- key judgements made in preparing the accounts
- any disputes arising between those preparing the accounts and the auditors
- reports, advice and findings from external audit (especially the Audit Completion Report – ISA 260 Report(September 2025))

Terms of reference

4.25 The committee's terms of reference should be agreed by the Accountable Officer/Board and made publicly available (including on the organisation's website). It is important that a balance is struck during meetings between corporate governance, risk management, control and financial reporting items. The terms of reference should be reviewed annually alongside the performance of the committee.

Model terms of reference are suggested at **Annex D**. A suggested self-assessment checklist is provided at **Annex J**.

4.26 The responsibilities assigned to the committee should not provide any conflict with the guidance in this handbook, in particular by compromising independence. The committee should not have any executive responsibilities or be charged with making or endorsing any decisions, although it may draw attention to strengths and weaknesses in control and make suggestions for how such weaknesses might be

dealt with. The overarching purpose of the committee is to advise the AO and Board; it is then the AO and Board that make the relevant decisions.

4.27 The committee should have appropriate authority to require any member of the organisation to report on the management of risk or on the control environment within their areas of responsibility, in general terms or in respect of specific issues, either by:

- attending a committee meeting
- providing written report(s) to the committee to help the committee in fulfilling its role

4.28 The AO and Board need adequate and timely feedback on the work of the committee in order to consider its contributions formally. A schedule of the committee's agreed delegations from the Board, and the mechanisms for feedback and assurance, should be formally documented.

4.29 To fulfil their role, most committees will need to meet at least four times a year. A model "core programme" of work for a Committee meeting four times a year is provided at **Annex E**.

4.30 The committee will require access to funding to cover the costs incurred in fulfilling its role. The funding should be sufficient to:

- meet any remuneration and working expenses of its members (where applicable)
- meet the relevant training needs of its members
- provide specialist (external) advice or opinions when required
- (as agreed with the organisation) provide external review of the effectiveness of the committee

Chapter 5: Communication and Reporting

Communication between the Committee and the Board

5.1 The work of the Audit and Assurance Committee needs to be effectively communicated. After each meeting of the committee a report should be prepared for the AO and Board to:

- summarise the business taken by the committee, explaining if necessary why that business was regarded as important
- offer the views of, and advice from, the committee on issues which they consider the Accounting Officer and Board should take action on

5.2 If the minutes of the committee meeting are used as the report, care should be taken in their presentation to highlight the advice being provided. These reports should be copied to the Head of Internal Audit and the External Auditor (especially if the report contains advice about, or to, the auditors).

Improving relationships

5.3 It is important for the committee to have good relationships and communication with those it seeks briefings from, and those it provides assurance to. This ensures that it is effectively engaged with the organisation and able to fulfil its function. This should include where risks cross organisational boundaries, for example, in major projects.

Annual reports

5.4 The committee should provide an Annual Report, timed to support the preparation of the Governance Statement. This internal report needs to be open and honest in presenting the committee's views if it is to be of real benefit to the AO and Board. This report is likely to be used by the AO and Board in preparing their own

report for publication in fulfilment of the reporting requirements of the Scottish Administration.

5.5 The Annual Report should summarise the committee's work for the prior year, and present its opinion about:

- the effectiveness of governance, risk management and control
- the comprehensiveness of assurances in meeting the AO's and Board's needs
- the reliability and integrity of these assurances
- whether the assurance available is sufficient to support the AO and Board in their decision taking and their accountability obligations

- the implications of these assurances for the overall management of risk
- any issues the committee considers pertinent to the Governance Statement and any long term issues the committee thinks the AO and/or Board should give attention to
- financial reporting for the year
- the quality of both Internal and External Audit and their approach to their responsibilities
- the committee's view of its own effectiveness, including advice on ways in which it considers it needs to be strengthened or developed

5.6 The Audit and Assurance Committee's report should take into account any other relevant assurance reports.

Bilateral communications

5.7 There should be mutual rights of access between the Chair of the Audit and Assurance Committee, the AO, Head of Internal Audit and the External Auditor. Periodic discussions outside of the formal meeting help to ensure that expectations are managed and that there is mutual understanding of current risks and issues.

Annex A: The role of the Chair: good practice

A1 Role of Chair

The role goes beyond chairing meetings and is key to achieving committee effectiveness. Key activities in addition to committee meetings should include the following.

- before each meeting, the Chair and the Committee Secretary (or equivalent role) should meet to discuss and agree the business for the meeting. The Chair should take ownership of, and have final say in, the decisions about what business will be pursued at any particular meeting
- meeting time should be optimised by making sure that all agenda papers are issued in good time and then having each paper summarised outlining the key points, cross referred to the organisational business and risk agenda and stating what action the committee is required to take
- the Chair should ensure that after each meeting appropriate reports are prepared from the committee to the AO and Board. An annual report to the AO and Board should also be provided
- the Chair should have bilateral meetings at least annually with the AO, the Head of Internal Audit and the External Auditor. In addition, the Chair should meet any people newly appointed to these positions as soon as practicable after their appointment
- the Chair should also ensure that all committee members have an appropriate programme of engagement with the organisation and its activities to help them understand the organisation, its objectives, business needs and priorities
- the Chair of the Audit and Assurance Committee should establish a mechanism enabling key stakeholders to consider the overall risk and assurance needs (see 5.3)

- encouraging good, open relationships between the committee, AO, Finance Director and Internal and External Auditors. There are a number of ways that a Chair can encourage this

The Chair should support and add weight to audit work by:

- promoting audit issues internally with relevant Board members and other directors to make sure they appreciate the value of audit
- holding managers within the organisation to account for the implementation of audit recommendations
- calling appropriate business heads to meetings, for example, to explain how they are delivering their agreed actions on risks for which they are responsible
- arranging separate meetings for the Chair, Non-Executives and independent members and Internal and External Auditors to help establish open working relationships
- arranging meetings with the Chair, Internal Auditors and the Finance Director etc. in the weeks leading up to the committee meeting to discuss areas for the agenda and papers that should be provided
- arranging meetings with the Internal Auditors (and possibly External Audit) immediately before the committee meeting to help give focus to discussions and
- the Chair should ensure that there is an appropriate process between meetings for action points arising from committee business to be appropriately pursued. The Chair should also ensure that members who have missed a meeting are appropriately briefed on the business conducted in their absence. Chairs may choose to rely on the Secretariat to take these actions

A.2 Appraisal

The Chair should take the lead in ensuring that committee members are provided with appropriate appraisal of their performance as a committee member and that

training needs are identified and addressed. The Chair should seek appraisal of their performance from the AO (or Chair of the Board, as appropriate).

The Chair should ensure that there is a periodic review (at least annually) of the overall effectiveness of the committee and of its terms of reference.

A.3 Appointments

The Chair should be involved in the appointment of new committee members, including providing advice on the skills and experience being sought by the committee when a new member is appointed.

A.4 Resources

The Chair is responsible for ensuring that the work of the committee is appropriately resourced.

Annex B: Committee support: good practice

B.1 The Secretariat should be able to support the Chair in identifying business to be taken, and the relevant priorities of the business. For this reason, and as the Audit and Assurance Committee is a committee of the Board, the Committee's Secretariat function should be supported by the Board Secretariat. The Chair of the committee and the Secretariat should agree procedures for commissioning briefing to accompany business items on the committee's agenda and timetables for the issue of meeting notices, agendas, and minutes. The Chair of the committee should always review and approve minutes of meetings before they are circulated.

B.2 The specific responsibilities of the Audit and Assurance Committee Secretariat should include:

- meeting with the Chair to prepare agendas for meetings
- commissioning papers as necessary to support agenda items
- circulating meeting documents in good time before each meeting
- arranging for executives to be available as necessary to discuss specific agenda items with the committee during meetings
- keeping a record of meetings and providing draft minutes for the Chair's approval
- ensuring action points are being taken forward between meetings
- support the Chair in the preparation of committee reports to the AO and Board
- arranging the Chair's bilateral meetings with the AO, the Head of Internal Audit, the External Auditor, and, in NDPBs, with the Chair of the Board etc
- keeping the Chair and members in touch with developments and relevant background information about developments in the organisation
- maintaining a record of when members' terms of appointment are due for renewal or termination
- ensuring that appropriate appointment processes are initiated when required
- ensuring that new members receive appropriate induction training, and that all members are supported in identifying and participating in ongoing training, and

- managing budgets allocated to the committee

B.3 When the committee decides to meet privately, the Chair should decide whether the Secretariat members should also withdraw. If so, the Chair should ensure that an adequate note of proceedings is kept supporting the committee's conclusions and advice.

Annex C: Model letter of appointment

It is recommended that the following issues be included in the Letter of Appointment of an Audit and Assurance Committee member.

Appointment and purpose

You are hereby appointed as a member of the Audit and Assurance Committee of (organisation). As a member of the committee, you are accountable to the Board (or AO where appropriate) through the Chair of the Committee. Your appointment is for (number) years from (date). This appointment may be renewed (number) times (by mutual agreement) after the duration of this appointment.

The committee is a committee of the Board of (organisation) and its purpose is to:

- review the comprehensiveness of assurances in meeting the assurance needs of the Board and AO
- review the reliability and integrity of these assurances
- review the integrity of the financial statements
- advise the Board and AO about how well assurances consequently support them in decision making and in discharging their accountability obligations

A copy of the committee's Terms of Reference is enclosed. The committee is chaired by (name) and the other members are (names). [It is recommended that new members be provided with a list of contact details.]

Support and training

The Secretary of the Committee is (name/contact details) and he/she will shortly be in touch with you to discuss and arrange appropriate induction training.

To help you understand the governance arrangements and the role of Audit and Assurance Committees in government, you should read the Audit and Assurance Committee Handbook published by the Scottish Government.

Commitment and remuneration

The committee should meet at least four times each year, but additional meetings may be required from time to time. You will also be expected to undertake appropriate training and activities designed to keep you in up to date with the organisation's activities and priorities. Your remuneration will be (include details of daily rate and procedures for claims and payment). All monies paid in connection with this appointment are taxable and it is your responsibility to make appropriate arrangements in respect of income tax.

Expenses and subsistence

Travel and subsistence costs will be paid in accordance with (*the organisation's*) standard arrangements. A copy of the current rates and conditions is enclosed for your information.

You are entitled to claim the following expenses and subsistence:

- travel expenses to and from home to the meeting venue
- travel and subsistence expenses incurred as part of the work of the committee

You would be entitled to travel standard class by rail. Any further clarification on (the organisation's) arrangements should be sought via the Secretary of the Committee. As a rule of thumb, the aim is to use the most efficient and economic means of travel, taking into account sustainability, subsistence costs and savings in time.

Conflicts of interest

Any potential conflict of interest for you in your committee role, including any arising from a change in personal circumstances during your period of appointment, must be considered on an ongoing basis. Depending on the nature of the business being discussed on the agenda potential conflicts should be declared to the Chair of the Committee.

Appraisal

As a member of the committee, you will be subject to appraisal by the Audit and Assurance Committee Chair (include brief details of the appraisal process).

Conduct

You are expected to conduct yourself in accordance with the principles of the Seven Principles of Public Life identified by the Committee on Standards in Public Life. A copy of the Seven Principles of Public Life is enclosed.

Liability

Under the terms of the “On-Board” issued by the Scottish Ministers, individual non-executive board members of public bodies and independent external members of board committees who have acted honestly and in good faith do not have to meet out of their own personal resources any personal civil liability which is incurred in the execution or purported execution of their board or committee functions, save where the person has acted recklessly.

Termination

If you choose to resign from this appointment, you will be expected to give (*number*) months’ notice, unless your circumstances have changed in a way that make it appropriate for you to resign immediately. If your performance as a committee member is decided to be unacceptable (see appraisal) or if your conduct (including conflicts of interests) is unacceptable your appointment may be terminated by the Board/AO (*delete as appropriate*).

Annex D: Model terms of reference

The Board (and/or AO - delete as appropriate) has established an Audit and Assurance Committee as a Committee of the Board to support in their responsibilities for issues of risk, control and governance and associated assurance through a process of constructive challenge.

Membership

The members of the committee are:

- non-executive directors: (List those who are appointed to the committee)
- independent external members: (List those who are appointed to the Audit and Assurance Committee; in all cases indicate the date of appointment and when the appointment is due to end/become eligible for renewal)

The committee will be Chaired by …….

The committee will be provided with a secretariat function by ……..

Reporting

The committee will formally report in writing to the Board and AO after each meeting. A copy of minutes of the meeting may form the basis of the report.

The committee will provide the Board and AO with an Annual Report, timed to support finalisation of the accounts and the governance statement, summarising its conclusions from the work it has done during the year.

Responsibilities

The committee will advise the Board and AO on:

- the strategic processes for risk, control and governance and the governance statement
- the accounting policies, the accounts, and the annual report of the organisation, including the process for review of the accounts prior to submission for audit, levels of error identified, and management's letter of representation to the external auditors
- the planned activity and results of both internal and external audit
- the adequacy of management response to issues identified by audit activity, including external audit's management letter/report
- the effectiveness of the internal control environment
- assurances relating to the corporate governance requirements for the organisation
- (where appropriate) proposals for tendering for either internal or external audit services or for purchase of non-audit services from contractors who provide audit services
- anti-fraud policies, whistle-blowing processes, and arrangements for special investigations

The Audit and Assurance Committee will also periodically review its own effectiveness and report the results of that review to the Board and AO.

Rights

The committee may:

- co-opt additional members for a period not exceeding a year to provide specialist skills, knowledge and experience
- procure specialist advice at the expense of the organisation on an ad-hoc basis to support particular committee business. Budgets for each procurement should be approved by the Board and/or AO

Access

The Head of Internal Audit and the representative of External Audit will have free and confidential access to the Chair of the Committee.

Meetings

The AAC shall be provided with a secretariat function by [name]

The procedures for meetings are:

- the committee will meet at least four times a year. The Chair of the Committee may convene additional meetings, as he/she deems necessary
- a minimum of (*number*) members of the committee will be present for the meeting to be deemed quorate
- committee meetings will normally be attended by the AO, the
    - Finance Director, the Head of Internal Audit, and a representative of External Audit (*add any others who may routinely attend such as representatives of sponsoring/sponsored bodies*)
- the committee may ask any other officials of the organisation to attend to assist it with its discussions on any particular matter
- the committee may ask any or all of those who normally attend but who are not members to withdraw to facilitate open and frank discussion of particular matters
- the Board or AO may ask the committee to convene further meetings to discuss particular issues on which they want the committee's advice

Information requirements

For each meeting, the committee will be provided with:

- a report summarising any significant changes to the organisation's Risk Register
- a progress report from the Head of Internal Audit summarising
    - work performed (and a comparison with work planned)

- key issues emerging from Internal Audit work
- management response to audit recommendations
- significant changes to the audit plan
- any resourcing issues affecting the delivery of Internal Audit objectives

- a progress report from the External Audit representative summarising work done and emerging findings

As and when appropriate, the committee will also be provided with:

- business update reports from the AO
- the Charter / Terms of Reference of the Internal Audit Directorate
- the Internal Audit Strategy
- the annual Internal Audit Plan
- the Head of Internal Audit's Annual Opinion and Report
- quality assurance reports on the Internal Audit function
- the draft accounts of the organisation
- the draft governance statement
- a report on any changes to accounting policies
- External Audit's management letter/report
- a report on any proposals to tender for audit functions
- a report on the Counter Fraud and Bribery arrangements and performance
- reports from other sources within the “three lines of assurance” integrated assurance framework (e.g. Best Value self-assessment Reviews, Gateway Reviews, Health Check Reviews, Major Digital Project Assurance Reviews,, Procurement Capability Reviews, Procurement Key Stage Reviews)

The above list suggests minimum requirements for the inputs which should be provided to the committee. In some cases more may be provided. N.B The Integrated Assurance framework previously carried out Digital Scotland Service

Standard reviews, however this is now the responsibility of the Senior Responsible Officer(s) within the Public Body. See guidance for details.

Annex E: Example Annual Core Work Programme

Standing items of business which should be routinely considered at each standard committee meeting:

- review performance relating to risk management
- consider any reports from Internal Audit and management responses
- consider financial reports, including relevant information about financial performance and achievement of financial targets
- consider any reports from other sources within the “three lines of assurance” integrated assurance framework

In addition, the following items are suggested as good practice aligned to business cycles for specific meetings throughout the year:

Spring Meeting

- review the Internal Audit charter / terms of reference, strategy and the periodic work plan for the coming financial year
- consider External Audit plans for the coming financial year

Summer Meeting

- review and consider the accounts for the financial year just finished
- consider (emerging) External Audit opinion for the financial year just finished
- review assurances provided by senior staff for the annual governance statement
- consider Internal Audit opinion for the financial year just finished
- consider an annual report on fraud and security
- advise the AO on signing the accounts and governance statement
- consider an annual report to the Board and AO

Autumn Meeting

- review the performance management arrangements adopted by the body including, where appropriate, the timetable for reviewing such arrangements
- consider the External Audit management letter for the previous financial year and the response to/implementation of any recommendations

Winter Meeting

- consider the committee's own effectiveness in its work
- review the committee's Terms of Reference

Annex F: Governing the internal audit function

From 1 April 2025 the Global Internal Audit Standards (GIAS) - accompanied by the Global Internal Audit Standards in the UK Public Sector Application Note – replaced the Public Sector Internal Audit Standards (PSIAS). Audit and Risk Assurance Committees will need to make sure that their internal audit arrangements are compliant with GIAS and that the head of internal audit provides an overall conclusion at least annually in support of wider governance reporting.

As noted within paragraph 4.15-SGAAC is the governing Committee in respect of the services DIAA provides to both core and shared service partners. However there are further conditions relevant to the IA function. Within GIAS, Domain III: Governing the Internal Audit Function outlines the Essential Conditions that must exist:

Authorised by the AAC

- discuss with the HIA and senior management the appropriate authority, role, and responsibilities of the IA function
- approve the IA charter, which includes the IA mandate and the scope and types of IA services
- champion the internal audit function and enable it to fulfil the purpose of IA and pursue its strategy and objectives

- work with senior management to enable the IA function's unrestricted access to the data, records, information, personnel, and physical properties necessary to fulfil the IA mandate
- support the HIA through regular, direct communication

Positioned independently

- demonstrate support by: specifying that the HIA reports to a level within the organisation that allows the IA function to fulfil the IA mandate; approving the IA charter, plan, budget and resource plan; making appropriate inquiries of senior management and the HIA to determine whether any restrictions in the IA function's scope, access, authority, or resources limit the function's ability to carry out its responsibilities effectively; meeting periodically with the HIA in sessions without senior management present
- establish a direct reporting relationship with the HIA and the IA function to enable the IA function to fulfil its mandate
- provide the HIA with opportunities to discuss significant and sensitive matters with the AAC, including meetings without senior management present
- engage with senior management and the HIA to establish appropriate safeguards if HIA roles and responsibilities impair or appear to impair the internal audit functions' independence
- engage with senior management to ensure that the IA function is free from interference when determining its scope, performing internal audit engagements, and communicating results

Overseen by the Board (where relevant)/SGAAC

- communicate with the HIA to understand how the internal audit function is fulfilling its mandate
- communicate the board's perspective on the organisation's strategies, objectives, and risks to assist the HIA with determining internal audit priorities

- set expectations with the HIA for: the frequency with which the board wants to receive communications from the HIA; the criteria for determining which issues should be escalated to the board, such as significant risks that exceed the board's risk tolerance; the process for escalating matters of importance to the board
- gain an understanding of the effectiveness of the organisation's governance, risk management, and control processes based on the results of internal audit engagements and discussions with senior management
- discuss with the HIA disagreements with senior management or other stakeholders and provide support as necessary to enable the HIA to perform the responsibilities outlined in the internal audit mandate
- discuss with the HIA, at least annually, the sufficiency, both in numbers and capabilities, of internal audit resources to fulfil the internal audit mandate and achieve the internal audit plan
- consider the impact of insufficient resources on the internal audit mandate and plan
- engage with senior management and the HIA on remedying the situation if the resources are determined to be insufficient
- approve the internal audit function's performance objectives at least annually. (In the DIAA context performance objectives are set by DIAA Director and then applied locally)
- assess the effectiveness and efficiency of the internal audit function - such an assessment includes:
    - reviewing the internal audit function's performance objectives including its conformance with the Standards, laws and regulations
    - ability to meet the internal audit mandate
    - progress towards completion of the internal audit plan
    - considering the results of the internal audit function's quality assurance and improvement programme

    - determining the extent to which the internal audit function's performance objectives are being met

- collaborate with senior management and the HIA to determine the scope and frequency of the external quality assessment (In DIAA context the commissioning, management and reporting of EQA is led by DIAA Director)
- consider the responsibilities and regulatory requirements of the internal audit function and the HIA, as described in the internal audit charter, when defining the scope of the external quality assessment (as above)
- require receipt of the complete results of the external quality assessment or self-assessment with independent validation directly from SGAAC (as above)
- review and approve the HIA's action plans to address identified deficiencies and opportunities for improvement, if applicable (as above)

Annex G: Key Questions for an Audit and Assurance Committee to Ask

This list of questions is not intended to be exhaustive or restrictive nor should it be treated as a checklist substituting for detailed consideration of the issues it raises. Rather it is intended to act as a set of "prompts" to help the committee ensure that their work is comprehensive.

On the strategic processes for risk, control and governance, how do we know:

- the risk management culture is appropriate
- there is a comprehensive process for identifying and evaluating risk, and for deciding what levels of risk are tolerable
- the risk register is an accurate reflection of the risks facing the organisation.
- appropriate ownership of risk is in place
- risk management is carried out in a way that really benefits the organisation or is it treated as a box ticking exercise

- the organisation as a whole is aware of the importance of risk management and of the organisation's risk priorities
- management has an appropriate view of how effective internal control is
- the system of internal control and effective risk identification and management will provide indicators of things that may be going wrong or off track
- the AO's annual governance statement is meaningful, and is underpinned by appropriate evidence
- the governance statement appropriately discloses action to deal with material problems
- the Board is appropriately considering the results of the effectiveness review underpinning the governance statement

On risk management processes, how do we know:

- how senior management (and Ministers where appropriate) support and promote effective risk management
- how well people are equipped and supported to manage risk well
- there is a clear risk strategy and policies
- the arrangements in place for identification and mitigation of risks are effective
- the organisation’s risk appetite has been articulated
- there are effective arrangements for managing risks with partners
- the organisation's processes incorporate effective risk management
- key strategic risks can be change quickly, scenario planning and stress testing can be carried out and “bubbling under” risks captured
- external and emerging risks are considered
- financial’ risks and “non-financial” risks are reviewed
- risk management contributes to achieving outcomes
- management are regularly reviewing top risks, including the effectiveness of mitigating actions

On the planned activity and results of both internal and external audit, how do we know:

- the Internal Audit strategy is appropriate for delivery of an informed assurance opinion on the whole of risk, control and governance
- the internal audit plan will achieve the objectives of the Internal Audit strategy, and in particular is it adequate to facilitate a positive, reasonable assurance on the key risks facing the organisation
- Internal Audit has appropriate resources, including skills, to deliver its objectives
- Internal Audit takes appropriate account of other assurance activity, especially in the first and second line (and that this assurance is understood and owned by management)
- Internal Audit recommendations that have been agreed by management are timeously implemented
- any issues arising from line management not accepting Internal Audit recommendations are appropriately escalated for consideration
- the quality of Internal Audit work is adequate. What does application of the Internal Audit Quality Assessment process tell us about the quality of the Internal Audit service
- there is appropriate access to both Internal and External Audit to discuss the organisations/Non-Executives assurance questions and concerns privately
- there is appropriate co-operation between the internal and external auditors
- External Audit's plan will provide sufficient scrutiny of the organisation's financial statements and assurance that resources have been discharged properly, effectively and efficiently
- the AO and Board have taken all necessary steps to make themselves aware of any relevant information and that auditors are aware of that information

On the accounting policies, the accounts, and the annual report of the organisation, how do we know:

- how effective and accurate budgeting and in-year forecasting is
- if the finance function is fit for purpose
- what the “hidden” financial risks are, relating to (inter alia):
    - HR
    - VAT
    - overruns
    - sudden loss of funding/revenue
- the accounting policies comply with relevant requirements, particularly the HMT Financial Reporting Manual
- there has been due process in preparing the accounts and annual report and is that process robust
- the accounts and annual report have been subject to sufficient review by management and by the Board and AO
- when new or novel accounting issues arise, appropriate advice on accounting treatment is sought and provided
- there is an appropriate anti-fraud policy in place and losses are suitably recorded
- suitable processes are in place to ensure accurate financial records are kept in line with legislative and organisational requirements
- suitable processes are in place to ensure fraud is guarded against, and regularity and propriety is achieved
- financial control, including the structure of delegations, enables the organisation to achieve its objectives with good value for money
- if there are any issues likely to lead to qualification of the accounts
- if the accounts have been qualified, that appropriate action is being taken to deal with the reason for qualification
- issues raised by the External Auditors are given appropriate attention

On the adequacy of management response to issues identified by audit activity, how do we know:

- the implementation of recommendations is monitored and followed up
- there are suitable resolution procedures in place for cases when management reject audit recommendations which the auditors stand by as being important

On assurances relating to the corporate governance requirements for the organisation, how do we know:

- corporate governance arrangements operate effectively and are clear to the whole organisation
- the AO's Governance Statement is meaningful, and that robust evidence underpins it
- the Governance Statement appropriately discloses action to deal with material problems
- the Board/Executive is appropriately considering the results of the effectiveness review underpinning the annual Governance Statement
- the range of assurances available is sufficient to facilitate the drafting of a meaningful annual Governance Statement
- those producing the assurances understand fully the scope of the assurance they are being asked to provide, and the purpose to which it will be put
- effective mechanisms are in place to ensure that assurances are reliable and adequately evidenced
- assurances are "positively" stated (i.e. – premised on sufficient relevant evidence to support them)
- the assurances draw appropriate attention to material weaknesses or losses which should be addressed
- the annual Governance Statement realistically reflects the assurances on which it is premised

On the work of the committee itself, how do we know:

- we are being effective in achieving our terms of reference and adding value to corporate governance and control systems of the organisation
- we have the appropriate skills mix
- we have an appropriate level of understanding of the purpose and work of the organisation
- we understand all of the sources of assurance available to the organisation
- we have sufficient time to give proper consideration to our business
- our individual members are avoiding any conflict of interest
- we are avoiding “group think”
- what impact we are having on an organisation

On the risk of cyber security, how do we know that:

- there is sufficient assurance that the organisation is properly managing its cyber risk, including having appropriate risk mitigation - does the committee have responsibility for review of the draft strategies
- the organisation has properly identified and evaluated the cyber security risk
- there are proper governance arrangements and controls to protect from, detect and respond to cyber security attacks/incidents (for example there is board member (or equivalent) with a specific security remit
- government expectations and standards relating to cyber security are considered and implemented within the organisation
- the organisation has suitably skilled and experienced staff, or access to such staff to deal with incidents
- there is suitable awareness and ongoing training within the organisation on the risk from cyber-attack

Annex H: Competency framework

All members of the committee should have, or acquire as soon as possible after appointment:

- understanding of the objectives of the organisation and current significant issues for the organisation
- understanding of the organisation's structure, including key relationships such as that with a sponsoring directorate/portfolio or a major partner
- understanding of the organisation's culture
- understanding of any relevant legislation or other rules governing the organisation
- understanding of the organisation’s three lines of assurance and sources of assurance
- broad understanding of the government environment, particularly accountability structures and current major initiatives
- understanding of responsibilities and expectations of the Board and Committee, regarding the support, check and challenge of the Internal/External Audit function
- understand the requirement to ensure the Internal/External audit functions are independent and qualified
- understanding of the Board’s role to ensure the Internal/External audit function is effective

The committee should collectively possess:

- knowledge/skills/experience (as appropriate and required) in:
    - accounting
    - risk management
    - audit
    - technical or specialist issues pertinent to the organisation's business
- experience of managing similar sized organisations and people management skills
- understanding of the wider relevant environments in which the organisation operates

- detailed understanding of the government environment and accountability structures

Annex I: Risk Control Framework

The Risk Control Framework, as updated in the May 2023 revision of the Orange Book, provides a structured approach to assessing and reporting on the effectiveness of governance, risk management and control arrangements across public sector organisations. Audit and Assurance Committees should ensure that their annual reporting reflects the principles and expectations set out in this framework.

Annual Reporting Requirements

The Audit and Assurance Committee's Annual Report should provide a clear and evidence-based opinion on the following:

- the effectiveness of governance, risk management and control arrangements, including the organisation's compliance with the updated Orange Book and its embedded Risk Control Framework
- the comprehensiveness of assurances in meeting the needs of the AO and Board
- the reliability and integrity of the assurances received
- whether the assurance available is sufficient to support the AO and Board in their decision-making and accountability obligations
- the implications of these assurances for the overall management of risk within the organisation
- any issues the committee considers pertinent to the Governance Statement, including long-term matters that should be brought to the attention of the AO and/or Board
- the quality of financial reporting for the year
- the quality and effectiveness of both internal and external audit functions and their approach to fulfilling their responsibilities

- the committee’s own effectiveness, including any recommendations for improvement or development

Group and Shared Service Considerations

Where risks span across a group of organisations or shared service arrangements, related Audit and Assurance Committees may be required to produce coordinated Annual Reports. These should be timed to support the production of any overarching governance or assurance reports and should reflect the collective risk and control environment.

Bilateral Communications

To support effective oversight and assurance, there should be mutual rights of access between the Chair of the Audit and Assurance Committee, the AO, the Head of Internal Audit, the Risk Manager (where this is a distinct function), and the External Auditor. Periodic bilateral discussions—at least annually—should be held outside of the formal committee structure to ensure expectations are aligned and there is a shared understanding of current risks and emerging issues.

Annex J: Self-assessment checklist

Prompts for self- assessment

Role and remit

Does the committee have written terms of reference?

Do the terms of reference cover the core functions identified in the handbook?

Are the terms of reference approved by the committee and reviewed periodically?

Has the committee been given enough membership, authority and resources to perform its role effectively and independently?

Does the governance statement mention the committee and its purpose?

Does the committee periodically assess its own effectiveness?

Membership, induction and training

Has the membership been formally agreed by the board or AO and has a quorum been set?

Are members appointed for a fixed term?

Does at least one member have a financial background?

Are all members, including the Chair, independent of the executive function?

Are new members provided with an appropriate induction?

Has each member formally declared their business interests?

Are members sufficiently independent of other key board committees?

Has the committee considered arrangements for assessing member attendance and performance?

Meetings

Does the committee meet regularly, at least four times a year?

Do the terms of reference set out the frequency and timing of meetings?

Does the committee calendar align with business and financial reporting needs?

Are members attending regularly, and is action taken where attendance is poor?

Does the AO attend meetings or receive a record if not?

Does the committee benefit from attendance by appropriate officials, including internal audit, external audit and finance?

Internal control

Does the committee consider findings from internal audit and others on the effectiveness of risk management, control and governance?

Does the committee consider reviews of the effectiveness of the system of internal control?

Does the committee review the draft governance statement separately from the accounts?

Does it consider how accurate and meaningful the governance statement is?

Does the committee confirm that arrangements for risk management, control and governance operated effectively during the reporting period?

Has the committee considered coordination with other committees responsible for risk and governance?

Has the committee satisfied itself that appropriate arrangements exist to prevent and deal with fraud?

Has the committee been made aware of the role of risk management in preparing the internal audit plan?

Do the terms of reference include oversight of risk management?

Does the committee consider assurances provided by senior staff?

Does it receive stewardship reports from key business areas such as finance, HR and IT?

Financial reporting and regulatory matters

Is the committee's role in reviewing the annual accounts clearly defined?

Does the committee consider the suitability of accounting policies and treatments?

Does it consider major judgements made?

Does it consider large write-offs?

Does it consider changes in accounting treatment?

Does it consider the reasonableness of accounting estimates?

Does it consider the narrative aspects of reporting?

Is there a meeting to receive and discuss the external auditor's report, including proposed adjustments and issues?

Does the committee review management's letter of representation?

Does the committee understand management's process for preparing the annual accounts?

Does it have a mechanism to stay aware of legal and regulatory issues?

Internal audit

Does the Head of Internal Audit attend committee meetings?

Does the committee review the internal audit plan annually and in detail, including coverage of key risks?

Does internal audit have a direct reporting line to the committee if required?

In addition to the annual report, does the committee receive progress reports from internal audit?

Are follow-up audits monitored and is implementation of recommendations reviewed?

Can the Chair hold private discussions with the Head of Internal Audit if needed?

Is there good cooperation between internal and external audit?

Does the committee review whether internal audit has adequate staffing and resources?

Are internal audit performance measures monitored?

Has the committee clarified what information it expects from internal audit?

Has the committee reviewed internal audit's formal terms of reference?

External audit

Does the external audit representative attend committee meetings?

Do the external auditors present and discuss their audit plans and strategy with the committee?

Does the Chair hold periodic private discussions with the external auditor?

Does the committee review the external auditor's annual report?

Does the committee ensure that actions on external audit recommendations are monitored?

Are reports on external audit work presented to the committee?

Does the committee assess the performance of external audit?

Does the committee consider the external audit fee?

Administration

Does the committee have a designated secretariat?

Are agenda papers circulated in advance to allow adequate preparation?

Do reports provide relevant information at the right time and in a useful format?

Does the committee provide guidance on the format and content of papers?

Are minutes prepared and circulated promptly to the right people?

Are matters arising tracked or raised at the next meeting?

Do action points clearly state who is responsible and by when?

Does the committee produce an effective annual report on its activities?

Overall

Does the committee contribute effectively to the organisation’s control environment?

Are there areas where the committee could improve its effectiveness?

Does the committee seek feedback from the Board and AO on its performance?

© Crown copyright 2026

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit **nationalarchives.gov.uk/doc/open-government-licence/version/3** or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: **psi@nationalarchives.gsi.gov.uk**.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at

The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-80775-243-9 (web only)

Published by The Scottish Government, August 2026

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS1749406 (08/26)

w w w . g o v . s c o t