

# Audit and Risk Assurance Committee Handbook

---



© Crown copyright 2025

This publication is licensed under the terms of the Open Government Licence v2.0 except where otherwise stated. To view this licence, visit [nationalarchives.gov.uk/doc/open-government-licence/version/3](https://nationalarchives.gov.uk/doc/open-government-licence/version/3).

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.uk/official-documents](https://www.gov.uk/official-documents).

Any enquiries regarding this publication should be sent to us at [public.enquiries@hmtreasury.gov.uk](mailto:public.enquiries@hmtreasury.gov.uk)

ISBN: 978-1-917151-23-8

PU: 3435

# Contents

<b>Foreword</b>	<b>4</b>
<b>Chapter 1 Introduction</b>	<b>5</b>
<b>Chapter 2 Good practice principles for Audit and Risk Assurance Committees</b>	<b>7</b>
<b>Chapter 3 Membership, independence, objectivity and understanding</b>	<b>9</b>
<b>Chapter 4 Skills</b>	<b>12</b>
<b>Chapter 5 The role and scope of the Committee</b>	<b>14</b>
<b>Chapter 6 Communication and reporting</b>	<b>22</b>
<b>Annex A The role of the Chair: good practice</b>	<b>24</b>
<b>Annex B Committee support: good practice</b>	<b>27</b>
<b>Annex C Example letter of appointment</b>	<b>29</b>
<b>Annex D Example terms of reference</b>	<b>32</b>
<b>Annex E Example core work programme</b>	<b>36</b>
<b>Annex F Key questions for an Audit and Risk Assurance Committee to ask</b>	<b>38</b>
<b>Annex G Competency framework</b>	<b>46</b>
<b>Annex H Governing the internal audit function</b>	<b>47</b>
<b>Annex I Audit and Risk Assurance Committee self-assessment checklist</b>	<b>51</b>

# Foreword

The “[Corporate governance in central government departments: Code of Good Practice](#)” guidance tasks organisational boards with setting the organisation’s risk appetite and ensuring that the framework of governance, risk management and control is in place. The Audit and Risk Assurance Committee (ARAC) plays a crucial role in supporting the board in meeting these obligations.

The ARAC role is a demanding one and requires strong and independent members with an appropriate range of skills and experience. It will benefit from a collaborative relationship with the organisation to ensure that the committee gets the support and information that it needs.

The ARAC should act as the conscience of the organisation, providing insight and constructive challenge where required, such as on risks arising from fiscal and resource constraints, new service delivery models, information flows on risk and control, and the agility of the organisation to respond to emerging risks.

The [2023 Orange Book – Management of Risk and Principles](#) introduced a risk control framework (RCF) for use by organisations to show that appropriate risk management processes exist. The RCF makes it easier for accounting officers to navigate and gain comfort on the existing internal control requirements contained in the functional standards, codes of conduct and guidance they are currently expected to adhere to. The 2023 Orange Book also introduces the requirement for each government organisation to either disclose compliance with the Orange Book or to explain their reasons for departure clearly and carefully in the Governance Statement accompanying their Annual Report and Accounts.

Whilst much of the content of this document focuses on central government departments, it is equally applicable to executive agencies, executive non-departmental public bodies and arm’s length bodies.

The changes to this updated handbook compared to the version published in July 2024 relate to the updated professional standards mandated for internal audit in the public sector. They took effect from 1 April 2025. Their impact on the role and scope of the Committee is detailed in Chapter 5 and **Annex H Governing the internal audit function**.

The checklist which an ARAC could use to review its effectiveness is now at **Annex I Audit and Risk Assurance Committee self-assessment checklist**

# Chapter 1

## Introduction

1.1 The government's Corporate governance in central government departments: code of good practice guidance (hereafter referred to as "the Code")

**Principle 5.1** provides that:

The board should ensure that there are effective arrangements for governance, risk management and internal control for the whole departmental family. Advice about and scrutiny of key risks is a matter for the board, not a committee. The board should be supported by:

- an Audit and Risk Assurance Committee (ARAC) chaired by a suitably experienced non-executive board member (NEBM);
- an internal audit service operating to the professional standards mandated for internal audit in the public sector; and
- sponsor teams of the department's key arm's length bodies (ALBs).

1.2 On ARACs, this principle is supported by six provisions in the Code.

- The board and accounting officer should be supported by an ARAC comprising of at least three members.
- Advising on key risks is a role for the board. The ARAC should support the board in this role.
- An ARAC should not have any executive responsibilities or be charged with making or endorsing any decisions.
- The board should ensure that there is adequate support for the ARAC; including a secretariat function. – **See Annex B Committee Support: Good Practice.**
- The ARAC should lead the assessment of the annual Governance Statement for the board.
- The terms of reference of the ARAC should be made available publicly.

1.3 The Code states "In addition to central government departments, the principles in the Code generally hold across other parts of central government, including departments' ALBs, which are encouraged to adopt the principles in the code wherever relevant and practical. Arrangements for ALBs may depend on statute. Generally, ministers do not chair boards of ALBs, or non-ministerial departments where statute sets out the applicable governance".

**This means that ARACs should be established in all departments, executive agencies, executive non-departmental public bodies and ALBs.**

1.4 Guidance to the Code recognises that the ARAC might be constituted as two separate committees:

- an audit committee, with a focus on assurance arrangements over: governance, financial reporting, annual report and accounts, including the governance statement and
- a risk committee, with a focus on ensuring there is an adequate and effective risk management and assurance framework in place.

In central government, all aspects would usually be covered by one committee, unless the anticipated workload or complexity of the business is such that one committee would not be able to provide sufficient attention. In such a case, some non-executive responsibilities in relation to risk might be more appropriately managed by a risk committee. Such a committee would typically focus on ensuring that the organisation is working within its risk appetite/tolerance and that the risk strategy is appropriately attuned to anticipated external conditions. It should be noted that the remit for any such committee should be clear and distinct from executive risk management committees that may already exist. The rest of this Handbook assumes that a single committee will be established (see **Annex D** for an example Terms of Reference).

1.5 The Code requires that the terms of reference of the ARAC including its role and the authority delegated to it by the board, should be made available publicly. The department should report annually on the work of the committee in discharging those responsibilities.

1.6 Any significant non-compliance with the five good practice principles of this Handbook (summarised in Chapter 2), taking account of the Code should be explained and reported to the board and if necessary be included in the Governance Statement.

## Chapter 2

# Good practice principles for Audit and Risk Assurance Committees

**This Handbook sets out five good practice principles for ARACs in central government. These are summarised below. Each principle is then further explained in the following chapters. Each principle is of equal importance.**

### Principle 1: Membership, independence, objectivity and understanding

The ARAC should be independent and objective; in addition, each member should be a non-executive, who should have a good understanding of the objectives and priorities of the organisation and of their role as an ARAC member.

### Principle 2: Skills

The ARAC should collectively own an appropriate skill mix to allow it to carry out its overall function and duties.

### Principle 3: The role of the ARAC

The ARAC should support the board and accounting officer 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.

### Principle 4: Scope of work

The scope of the ARAC work should be defined in its terms of reference and encompass all the assurance needs of the board and accounting officer. Within this, the ARAC should have particular engagement with the work of internal audit, risk management, external audit, counter fraud and financial management and reporting issues.

## Principle 5: Communication and reporting

The ARAC should ensure that it has effective communication with all key stakeholders, for example, the board, the head of internal audit, the external auditor, the risk manager and other relevant assurance providers such as the counter fraud manager.



# Chapter 3

## Membership, independence, objectivity and understanding

**Principle 1: The ARAC should be independent and objective; in addition, each member should be a non-executive, who should have a good understanding of the objectives and priorities of the organisation and of their role as an ARAC member.**

### Independence

**3.1** An effective ARAC must have members who are independent and objective. The board and accounting officer should be supported by an ARAC with no executive responsibilities, comprising at least three non-executive members.

**3.2** The Chair of the committee should be a non-executive board member (NEBM<sup>1</sup>) with relevant experience. There should be at least one other NEBM on the committee (but to retain independence, the chair of the board should not be a member of ARAC). The committee can seek further independent, non-executive membership from sources other than the board, in order to ensure an appropriate level of skills and experience. NEBM recruitment is regulated by The Commissioner for Public Appointments and should be undertaken in line with Cabinet Office guidance ([Governance Code on Public Appointments](#)) on the recruitment, appointment and development of non-executive members of Civil Service boards. 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).

### Relationship with the Executive

**3.3** Executive members of the organisation should not be appointed to the ARAC. The role of the Executive is to attend, to provide information, and to

---

<sup>1</sup> NEBMs are required for departmental boards. Their equivalents in ALBs may be referred to as Non-Executive Directors

participate in discussions, either for the whole duration of a meeting or for particular items.

**3.4** The accounting officer and the finance director should routinely attend ARAC meetings. It is also normal for the head of internal audit, risk manager and a representative of the external auditor to attend each meeting. However, the terms of reference should also provide for the ARAC to meet privately without any non-members present for all, or part, of a meeting if they so wish.

**3.5** It is also good practice:

- for the Chair of the ARAC to meet separately with the accounting officer, the finance director, the head of internal audit and the external auditor's senior representative outside of the formal committee structure (see paragraph 6.7).
- for other ARAC members (if leading on areas of work for the committee) to keep in touch with relevant staff outside of the formal meetings.

**See Annex A for good practice points for the role of the Chair.**

## Other participants

**3.6** For some ALBs there may be significant overlap or homogeneity of function, for example, covering different remits/regions, or an ALB may represent a large or important element of a department's remit or expenditure. In such cases, it may prove more efficient and effective (as well as helping to promote group working across departmental families) to establish shared ARAC arrangements or to have membership crossover in the separate committees across the department, avoiding conflicts of interest. For example, ARAC members of ALBs may be members of the Departmental ARAC.

**3.7** Sponsoring departments and their ALBs should ensure that the inter-relationship, including any cross-attendance of ARACs is agreed and appropriately documented in the Framework Document (using the inter-relationship of accountabilities at the accounting officer level as a guiding factor). Attention should be given to the processes by which information and assurance is communicated between ARACs, in particular regarding assurance necessary to support the departmental Governance Statement.

**3.8** Where there is no significant overlap of duties between the ALB and Department, consideration should be given to having a senior member of departmental staff attending the ALB ARAC to ensure the sponsor department is aware of key governance processes and issues within ALBs.

## Conflicts of interest

**3.9** Normally the process for recording declarations of conflicts of interests in the ARAC should mirror the processes used at board level. Each member of the committee should take personal responsibility to declare pro-actively any potential conflict of interest arising out of business undertaken by the organisation(s), arising on the committee's agenda or from changes in the

member's personal circumstances. The Chair of the committee 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; or in more extreme cases the member could be asked to stand down from the committee. If it is the Chair who has a conflict of interest, the board 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 extent and duration of the conflict of interest: a conflict likely to endure for a long time is more likely to suggest that the member should stand down.

## Terms of appointment

**3.10** All members of the ARAC 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 ARAC membership;
- the duration of their appointment and how often it may be renewed. Cabinet Office guidance [Governance Code on Public Appointments](#) for appointment of an NEBM is that the first appointment is for a fixed three years which can be renewed for up to three years, hence a maximum of six years; and
- training required and how this will be provided.

**3.11** The terms of appointment of an ARAC member should be clearly set out at the time of appointment. An example letter of Appointment is set out at **Annex C**. The letter should also specify what other activities (outside the NEBM role) the individual may or may not undertake in relation to the organisation. The impact on independence of remuneration from other activities should be given careful consideration. More detailed guidance on the making of appointments can be found in [Governance Code on Public Appointments](#).

# Chapter 4

## Skills

**Principle 2: The ARAC should collectively own an appropriate skill mix to allow it to carry out its overall function and duties.**

### Range of skills

4.1 The ARAC is charged with ensuring that the board and accounting officer of the organisation gain the assurance they need on governance, risk management, the control environment and on the integrity of the financial statements, as well as other elements of the annual report and accounts. It therefore needs a good range of skills and experience in relation to governance, risk, control and financial management. Because of the importance of financial management and reporting to every organisation, at least one member of the committee should have recent and relevant financial experience sufficient to allow them to competently analyse the financial statements and understand good financial management disciplines or any complex financial transactions of the organisation.

4.2 The ARAC should identify and agree with the board, the other skills required for committee effectiveness. These wider skills may be in relation to the core business of the organisation, or related to key developments, for example relating to change management or IT where this is of strategic significance to the organisation. The required skill set should be periodically reviewed (every two to three years).

4.3 As the ARAC matures, the skills and knowledge of the members should also develop, enabling them to focus on the key issues facing the organisation. ARAC networking or conferences within and across departmental boundaries can be a good way to keep up with current developments which may affect the organisation.

4.4 Although ARAC members are recruited for their individual skills, it is vital that they are able to work collaboratively.

### Additional skills

4.5 The ARAC should be empowered to both:

- co-opt members (complementing the three standing members) for a period of time (not exceeding a year and with the approval of the board)

to provide specialist skills, knowledge and experience, which the committee needs at a particular time; and

- procure specialist advice at the expense of the organisation on an ad-hoc basis to support them in relation to particular pieces of committee business.

## Training and development

**4.6** All ARAC members, whatever their status or background, will have training and development needs, especially for recent developments or emerging risk areas (e.g. artificial intelligence). Those who have recently joined the ARAC will need induction training, to help them understand their role and/or the organisation. Those joining a public sector ARAC for the first time with no experience of government will need training to help them understand the public sector accountability framework, especially those elements relating to governance and accountability. The Government Internal Audit Agency run regular training sessions for ARAC members.

**4.7** The committee 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.

**4.8** **Annex G** provides a suggested Competency Framework for ARAC members.

# Chapter 5

## The role and scope of the Committee

**Principle 3: The ARAC should support the board and accounting officer 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.**

**Principle 4: The scope of the ARAC work should be defined in its terms of reference and encompass all the assurance needs of the board and accounting officer. Within this, the ARAC should have particular engagement with the work of internal audit, risk management, external audit, counter fraud and financial management and reporting issues.**

### Supporting the accounting officer and the board

**5.1** Accounting officers and boards have many issues competing for their attention. One of the challenges they face is knowing if they are giving their attention to the right issues. Key to addressing this is assurance, which draws attention to the aspects of governance, risk management and control that are functioning effectively and, just as importantly, the aspects which need to be given attention to improve them.

**5.2** The accounting officer and board are responsible for developing an effective governance, risk management and control framework. A risk-based approach to assurance helps the accounting officer and board to judge if its agenda is focussing on the issues that are most significant in relation to achieving the organisation's objectives and strategy and if best use is being made of resources.

**5.3** The ARAC supports the accounting officer and board to formulate their assurance needs, by reviewing risks, systems and processes and considering how well the assurance provided actually meets these needs. ARACs should gauge the extent to which assurance on the management of risk 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 resources at its

disposal, targeting areas of greatest risk. This can include carrying out a “deep dive” exercise of risks that the committee determine are key threats to the organisation.

**5.4** 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; and
- 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 governance, risk management and control in accordance with the professional standards mandated for internal audit in the public sector.

**5.5** A well-designed assurance framework should identify all the key sources of assurance in the organisation and seek to coordinate 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 model’. By defining the sources of assurance in three broad categories, it helps to understand how the type and nature of the mechanisms can contribute to the bigger assurance picture:

- a) First line: management assurance from “front line” or business operational areas;
- b) Second line: oversight of management activity, separate from those responsible for delivery, but not independent of the organisation’s management chain (such as a quality assurance function); and
- c) Third line: independent and more objective assurance, including the role of internal audit and from external bodies (e.g., accreditation and Gateway reviews). Further detail of the work of internal audit is provided later in this chapter.

**5.6** An understanding of the three lines model can help the ARAC to play a key role in helping the accounting officer and board establish an optimal mix of assurance. [The 2023 Orange book](#), part 2 defines assurance and provides clarity on controls assurance aspects of existing guidance by introducing a Risk Control Framework (RCF), including a supporting bank of questions covering all aspects of the RCF, standards, codes and guidance applicable to accounting officers.

**5.7** The overall provision of assurances to the accounting officer and board should be reviewed by the ARAC, which should constructively challenge:

- if the nature and scope of the assurance providers’ activity meets the accounting officer and board’s assurance needs;

- the credibility and independence of each provider; and
- where appropriate, the actual assurances to test that they are founded on sufficient reliable evidence and that conclusions are reasonable in the context of the evidence.

**5.8** The ARAC should proactively commission assurance work from appropriate sources if it identifies any significant governance, risk management and control issues, which are not being subjected to sufficient review. ARACs should also seek assurance that weaknesses identified by reviews that have been conducted are remedied by management.

**5.9** A list of questions for ARACs to consider asking on key areas of their responsibility is provided at **Annex F**.

**5.10** The ARAC should draw the board's attention to areas where:

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

**5.11** In accordance with the [Code](#), assurance should be obtained on risks across the departmental family/group. The 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.

**5.12** Similarly, assurance on risk and control should also encompass services outsourced to external providers, including shared service arrangements, so that all key elements of the organisation are considered.

**5.13** 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 ARAC Forum, which meets, for example, twice a year. The Group would focus on assurances on cross organisational governance, risk and control arrangements. [The National Audit Office publication Cross-Government working: good practice](#) provides useful guidance in this area.

## Internal and external audit

**5.14** For any government organisation there will always be two significant sources of independent and objective assurance: internal audit and external audit.

**5.15** The work of internal audit is carried out primarily for the benefit of the accounting officer and board of the organisation and is likely to be the single most significant resource used by the ARAC in discharging its responsibilities. This is because the head of internal audit, in accordance with the professional



standards mandated for internal audit in the public sector, must prepare an overall conclusion at least annually that encompasses the adequacy and effectiveness of the organisation's governance, risk management and control processes.

**5.16** The [Global Internal Audit Standards \(GIAS\)](#) that have been mandated for use in the UK the public sector contain '*Essential Conditions*' in Domain III: 'Governing the Internal Audit Function'. The Essential Conditions are actions that ARACs should take to support the effective conduct of internal audit and successful implementation of GIAS in their organisation and these are collated in **Annex H**.

**5.17** The role of the ARAC in relation to internal audit includes approval of the internal audit mandate, charter, plan, budget, and resource plan.

**5.18** The ARAC should advise the accounting officer and the board on:

- how well the internal audit mandate, charter, plan, strategy and resource plan reflect the organisation's strategic objectives, risk exposure and support the head of internal audit's responsibility to provide an overall conclusion at least annually;
- the adequacy of the financial, human and technological resources available to 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;
- results of any cross government internal audit work;
- the annual internal audit overall conclusion and annual report;
- the performance of internal audit, including conformance with the applicable standards, expected performance measures, and the results of both internal and external quality assurance assessments, which should be reported to the ARAC by the head of internal audit; and
- the implementation status of internal audit recommendations.

**5.19** In central government, the National Audit Office under the Comptroller and Auditor General is responsible for external audit. Although the work of external audit is normally primarily conducted for the benefit of Parliament, it is still of significant benefit to the organisation. The ARAC should consider:

- the results of external audit work and resolution of identified weaknesses;
- the external auditor's planned audit approach and performance to date and if this is adequate;
- the way in which the external auditor is co-operating with internal audit to maximise overall audit efficiency, capture opportunities to derive a greater level of assurance and minimise duplication of work;

- the potential implications to the organisation of the wider work carried out by the external auditor, for example, value for money reports and good practice findings;
- the letter of representation to the external auditor at the end of the year, to ensure ARAC is aware of the key areas within the letter, or to discuss those issues which have not been previously reported to ARAC or are unusual; and
- whether the level of fees is appropriate for work to be undertaken.

**5.20** Separate meetings between ARAC members and internal and external auditors should be held (at least annually) to help the non-executives establish open working relationships and provide auditors the opportunity to discuss any issues of concern.

## Governance and the control environment

**5.21** It is essential that the ARAC understands how governance and internal control arrangements support the achievement of the department's strategies and objectives, especially:

- the board operating framework, including the department'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; and
- relations with ALBs/Sponsor Department.

## Risk management

**5.22** It is also essential that the ARAC:

- understands the organisation's business strategy, operating environment and the associated risks, taking into account all key elements of the organisation as part of a departmental family;
- understands the role and activities of the board (or equivalent senior governance body) in relation to managing risk and impact on the work of ARAC;

- 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, without second guessing management, to provide assurance that the arrangements are actively working in the organisations;
- critically challenges and reviews the adequacy and effectiveness of control processes (including risk registers) in responding to risks within the organisation's governance, operations, compliance and information systems, including undertaking deep dives into significant risks; and
- considers whether the risk management system will be effective in identifying new and emerging risks.

The [Orange book: Management of risk – principles and concepts](#) should be used to manage risks.

## Counter fraud

**5.23** The ARAC should consider counter fraud arrangements on a regular basis to understand the main fraud and error risks and management actions to mitigate these. They should satisfy themselves that:

- there is an appropriate anti-fraud policy in place which is regularly reviewed and updated;
- suitable processes are in place to ensure fraud is guarded against (i.e., controls are designed to prevent and detect fraud and error);
- losses are suitably recorded and responded to; and
- quarterly returns on counter fraud are made to the Cabinet Office.

**5.24** The ARAC should get reports on major incidents and near misses as well as details of special investigations, including any whistleblowing cases.

## Financial management and reporting

**5.25** The ARAC should consider significant accounting policies (guidance can be found in [HM Treasury's Financial Reporting Manual](#)), 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.

**5.26** The ARAC will not itself be able to review the accounts in detail to advise the accounting officer whether they are true and fair. Ideally, the committee should expect a comprehensive overview of the financial statements by the

finance director, 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, especially if there have been any changes to accounting standards;
- 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; and whether specialist advice was obtained when required;
- any disputes arising between those preparing the accounts and the auditors; and
- advice and findings from external audit (especially the Audit Completion Report – ISA 260 Report).

**5.27** The ARAC should also consider the contents of the Annual Report to ensure this is reasonable and in accordance with ARAC's understanding of the organisation.

## Terms of reference

**5.28** The ARAC's terms of reference should be agreed by the 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 regularly alongside the performance of the ARAC. An example Terms of Reference for an ARAC is suggested at **Annex D**.

**5.29** The responsibilities assigned to the ARAC should not provide any conflict with the guidance in this handbook, in particular by compromising independence. An ARAC 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 mitigated. The overarching purpose of the ARAC is to advise the board; it is then the board that makes the relevant decisions.

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

- attending an ARAC meeting; or
- providing written report(s) to the ARAC for the purpose of providing information to assist the committee in fulfilling its role.

5.31 The board needs adequate and timely feedback on the work of the ARAC 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 documented in the board operating framework.

5.32 To fulfil its role, the ARAC should meet at least four times a year, scheduled to align with the audit and assurance cycle. An example "core programme" of work for an ARAC meeting four times a year is provided at **Annex E**.

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

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

# Chapter 6

## Communication and reporting

**Principle 5: The ARAC should ensure that it has effective communication with all key stakeholders, for example, the board, the head of internal audit, the external auditor, the risk manager and other relevant assurance providers, such as the counter fraud manager.**

### Communication between the committee and the board

6.1 The work of the ARAC needs to be effectively communicated, including across the departmental group. After each meeting of the committee a verbal or written report should be provided to the board and accounting officer to:

- summarise the business taken by the committee, explaining, if necessary, why that business was regarded as important; and
- offer the views of, and advice from, the committee on issues which they consider the board or accounting officer should be taking action.

6.2 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.

6.3 It is important for the ARAC to have good relationships and communication with those it seeks briefings from, and those it provides assurance to. This ensures that the committee 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 (see 5.13).

### Annual reports

6.4 The ARAC 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 board and accounting officer. This report is likely to be used by the board in preparing its own report for publication in fulfilment of the reporting requirements of the [Code](#).

**6.5** The Annual Report should summarise the ARAC's work for the year past, and present the committee's opinion about:

- the effectiveness of governance, risk management and control; specifically including the organisation's proposed disclosure on compliance with [the Orange Book](#) updated in May 2023 and which now includes the Risk Control Framework;
- the comprehensiveness of assurances in meeting the board and accounting officer's needs;
- the reliability and integrity of these assurances;
- if the assurance available is sufficient to support the board and accounting officer in their decision taking and their accountability obligations;
- the implications of these assurances for the overall management of risk;
- any issues the ARAC considers pertinent to the Governance Statement and any long-term issues the committee decides should draw the board and/or accounting officer attention;
- financial reporting for the year;
- the quality of both internal and external audit and their approach to their responsibilities; and
- the committee's view of its own effectiveness, including advice on ways in which it considers it needs to be strengthened or developed.

**6.6** The ARAC's opinion should take into account any other relevant assurance reports. For example, where there are risks across a group, related committees may need to produce Annual Reports along the lines of 6.5 above, timed to support the production of the overarching group report.

## Bilateral communications

**6.7** There should be mutual rights of access between each of the Chair of the ARAC, the accounting officer, risk manager (if a separate function), head of internal audit and the external auditor. Periodic discussions (at least annually) 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

**A.1** The role of the Chair of the ARAC goes beyond chairing meetings. Indeed, it is key to achieving committee effectiveness. Activities in addition to committee meetings should include the following.

- Agreeing a draft forward workplan for the committee, at the start of each financial year, to ensure all matters which the committee is responsible for, will be properly considered throughout the year and at the right time.
- Before each meeting, the Chair and the Committee Secretary should meet to discuss and agree the business for the meeting, including time allowed 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 (in writing or verbal) are prepared from the ARAC to the board. A written annual report to the board should also be provided.
- The Chair should have bilateral meetings (at least annually) with the accounting officer, the head of internal audit, risk manager and the external auditor, and in Non-Departmental Public Bodies (NDPBs), with the Chair of the Departmental Board. 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.
- In a Departmental family or Group environment, the Chair of the Department or Group ARAC should establish a mechanism enabling key



stakeholders to consider the Department's or group's overall risk and assurance needs.

- Encouraging good, open relationships between the ARAC, accounting officer, finance director, risk manager and internal and external auditors.
- The Chair should support and add weight to audit work by:
  - a) promoting audit issues internally with relevant board members and other directors to demonstrate the value of audit;
  - b) holding managers within the organisation to account for the implementation of all audit recommendations; and
  - c) 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, independent members and internal and external auditors to help non-executive members establish open working relationships.
- Arranging meetings with the Chair, internal auditors, the finance director and risk manager in the period 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 and the risk manager) immediately before the ARAC meeting to help give focus to discussions.
- 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.
- Consider ways in which to obtain feedback from stakeholders (e.g., internal and external audit as well as executives) on the performance of the ARAC.

## Appraisal

**A.2** 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 met. The Chair should seek appraisal of their own performance from the accounting officer (or Chair of the Board, as appropriate).

**A.3** The Chair should ensure that there is a periodic review (at least annually) of the overall effectiveness of the ARAC and of its terms of reference. See **Annex I**.

The Chair may consider commissioning an external review at their discretion. The Chair shall ensure any areas of concern from the reviews are considered and actioned.

## Appointments

**A.4** The Chair shall 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. The Chair should consider how to map the skills required, those skills already in place and the skills gaps to be filled.

**A.5** The Chair should also be actively involved in the appointment of the head of internal audit.

## Resources

**A.6** 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 of the committee in identifying committee business to be taken and the relevant priorities of the organisation. The Chair of the committee and the secretariat should agree procedures for commissioning briefings to accompany items on the committee's agenda and timetables for issuing 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 ARAC Secretariat should include:

- meeting with the Chair of the committee to prepare agendas for meetings;
- commissioning papers as necessary to support agenda items;
- circulating 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 and circulating minutes promptly;
- ensuring action points are being taken forward between meetings and providing an update on these at each meeting;
- support the Chair in the preparation of ARAC reports to the board;
- arranging the Chair's bilateral meetings with the accounting officer, the head of internal audit, risk manager and the external auditor, and, in NDPBs, with the Chair of the Board;
- keeping the Chair and members in touch with developments in the organisation, (including providing relevant background information);
- maintaining a record of when members' terms of appointment are due for renewal or termination;

- ensuring appropriate appointment processes are initiated as required;
- ensuring new members receive appropriate induction training, and all members are supported in identifying and participating in ongoing training; and
- managing budgets allocated to the ARAC.

**B.3** When the ARAC 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

## Example letter of appointment

**It is recommended that the following areas be included in the Letter of Appointment of an ARAC member.**

### Appointment and purpose

You are hereby appointed by the [board / accounting officer (*delete as appropriate*)] as a member of the Audit and Risk Assurance Committee (ARAC) of [organisation]. As a member of the ARAC you are accountable to the [board / accounting officer] 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 ARAC is a committee of the board of [organisation] and the purpose of the ARAC is to:

- review the comprehensiveness of assurances on governance, risk management and the control in meeting the board and accounting officer's assurance needs;
- review the reliability and integrity of these assurances;
- review the integrity of the financial statements and annual report; and
- advise the board and accounting officer about how well assurances support them in decision-taking and in discharging their accountability obligations.

A copy of the ARAC's Terms of Reference is [enclosed / can be found here (add link to web page) (*delete as appropriate*)]. The committee is chaired by [name] and the other members are [names]. [It is recommended that the new member be provided with a list of committee member contact details]

## Support and training

The Secretary of the ARAC is [name / contact details] and they 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 the ARAC in government, copies of **“Corporate governance in central government departments: Code of good practice”** and HM Treasury **“Audit and Risk Assurance Committee Handbook”** are also enclosed with this letter of appointment/can be found here (add links to web page) *(delete as appropriate)*.

## Commitment and remuneration

Your duties as an ARAC member are expected to typically take [number] days per annum, including time to read papers in preparation for meetings and a programme of activity to keep you in touch with the organisation’s activities and priorities. The committee normally meets [number] times each year, but additional meetings may be required from time to time. Your remuneration will be *[include details of amount and means by which it will be paid]*.

## Travel 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 travel and subsistence expenses incurred as part of the work of the committee, including travel expenses to and from home to the meeting venue. You are entitled to travel standard class by rail, but the aim is to use the most efficient and economic means of travel, taking into account sustainability, subsistence costs and savings in time.

Any further clarification on [the organisation’s] arrangements should be sought via the Secretary of the committee.

## Conflicts of interest

You are required to register any interests you have. If during your period of appointment to the ARAC, your personal circumstances change in any way that may provide a conflict of interest for you in your ARAC role, you are to declare the circumstances to the Chair of the ARAC.

## Appraisal

As a member of the ARAC you will be subject to appraisal by the ARAC Chair *[include brief details of the appraisal process]*.

## Conduct

Although your appointment does not make you a Civil Servant, you are expected to conduct yourself in your role in government in accordance with the **Seven Principles of Public Life**. A copy [is enclosed / can be found here (add link to web page) *(delete as appropriate)*].

## 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 an ARAC member is decided to be unacceptable or if your conduct (including conflicts of interests) is unacceptable your appointment may be terminated by the [board / accounting officer].

# Annex D

## Example terms of reference

**The board has established an Audit and Risk Assurance Committee (ARAC) as a committee of the board to support them in their responsibilities for governance, risk management and control by reviewing the comprehensiveness of assurances in meeting the board and accounting officer's assurance needs and reviewing the reliability and integrity of these assurances.**

### Membership

The members of the ARAC are:

- non-executive board members: [list those who are appointed to the ARAC].
- independent External members: [list those who are appointed to the ARAC; in all cases indicate the date of appointment and when the appointment is due to end / become eligible for renewal)

The ARAC shall be chaired by [name].

### Reporting

- The ARAC shall formally report (either verbally or in writing) to the board and accounting officer after each meeting.

The ARAC shall provide the board and accounting officer with a written Annual Report, timed to support finalisation of the accounts and the Governance Statement, summarising its conclusions on the effectiveness of the control framework in place from the work it has done during the year.

### Responsibilities

The ARAC shall approve the internal audit mandate, charter, plan, budget and resource plan. See **Annex H**

The ARAC shall advise the board and accounting officer on:



- the strategic processes for governance, risk management and control 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;
- adequacy of management response to issues identified by audit activity, including external audit's management letter;
- assurances relating to the management of risk and corporate governance requirements for the organisation;
- the effectiveness of the internal control environment;
- (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, whistleblowing processes, and arrangements for special investigations; and
- the ARAC shall also periodically review (at least annually) its own effectiveness and report the results of that review to the board. The Chair may consider commissioning an external review if considered necessary. See **Annex I** for a self-assessment checklist.

## Rights

The ARAC may:

- co-opt additional members for a period not exceeding a year to provide specialist skills, knowledge and experience;
- procure specialist ad-hoc advice at the expense of the organisation, subject to budgets agreed by the board.

## Access

The head of internal audit and the representative of external audit shall have free and confidential access to the Chair of the ARAC.

## Meetings

- The ARAC shall be provided with a secretariat function by [name];

- The ARAC shall meet at least four times a year. The Chair of the ARAC may convene additional meetings, as they deem necessary;
- A minimum of [number] members of the ARAC shall be present for the meeting to be deemed quorate;
- ARAC meetings will normally be attended by the accounting officer, the finance director, risk manager, 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 ARAC may ask any other officials of the organisation to attend to assist it with discussions on any particular matter;
- The ARAC 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; and
- The board or the accounting officer may ask the ARAC to convene further meetings to discuss particular issues on which they want the committee's advice.

## Information requirements

**For each meeting, unless otherwise agreed, the ARAC shall be provided (at an agreed time in advance of the meeting) with:**

- a report summarising any significant changes to the organisation's strategic risks and a copy of the strategic/corporate Risk Register;
- a progress report (written or verbal) from the head of internal audit summarising:
  - a) work performed (and a comparison with work planned);
  - b) key issues emerging from the work of internal audit;
  - c) management response to audit recommendations;
  - d) changes to the agreed internal audit plan for ARAC approval; and
  - e) any resourcing issues affecting the delivery of the objectives of internal audit;
- a progress report (written or verbal) from the external audit representative summarising work done and emerging findings (this may include, where relevant to the organisation, aspects of the wider work carried out by the National Audit Office, for example, Value for Money reports and good practice findings);

- management assurance or changes to the control environment reports; and
- reports on the management of major incidents, “near misses” whistleblowing cases and lessons learned.

**As and when appropriate the committee shall also be provided with:**

- proposals for the review of terms of reference of internal audit / the internal audit mandate and charter;
- the internal audit strategy;
- the head of internal audit’s annual overall conclusion and report;
- quality assurance reports on the internal audit function;
- the draft annual report and accounts of the organisation;
- the draft Governance Statement;
- a report on any changes to accounting policies;
- external audit’s management letter;
- a report on any proposals to tender for audit functions;
- an update on co-operation between internal and external audit;
- the organisation’s Risk Management strategy and
- relevant reports from any other assurance providers, for example Gateway reviews.

*The above list suggests minimum requirements for the inputs which shall be provided to the ARAC. In some cases, more may be provided. For instance, it might be agreed that ARAC members should be provided with a copy of the report of every internal audit assignment.*

# Annex E

## Example core work programme

### Standing Items for each meeting

- Review the organisation's strategic risk register and risk management processes (including compliance with the Orange Book) put in place by the executive team and consider undertaking deep dives into specific risks.
- Consider the Head of Internal Audit's update and any individual reports, as required.
- Consider any reports from other sources of assurance.

### Spring Meeting

- Consider progress/planning for the annual report and accounts.
- Consider the external audit update report (findings for the current year and plans for their review of annual report and accounts).
- If available, consider / advise on the contents of the (draft) Governance Statement for the financial year just ended.
- Review and approve the internal audit mandate, charter, terms of reference, periodic work plan, budget, and resource plan for the coming financial year.
- Consider counter fraud work plans for the coming year, including ensuring a review of the counter fraud strategy and policy for the organisation.
- Consider the committee's own effectiveness.

### Summer Meeting

- Review and consider the annual report and accounts (particularly the annual Governance Statement) and advise the accounting officer who is responsible for signing them.
- Consider the (emerging) External Audit opinion and findings on the annual report and accounts.

- Consider Head of Internal Audit annual report and annual overall conclusion.
- Consider annual reports on counter fraud, whistleblowing and conflicts of interest.
- Agree the ARAC's annual report to the board.

Some ARACs choose to have an additional separate meeting timed to deal with the pre-recess finalisation of the annual report and accounts.

### Autumn Meeting

- Consider the external audit management letter for the previous financial year and the response to / plans for implementation of any recommendations.
- Consider the external audit strategy proposed in respect of current year's annual report and accounts.

### Winter Meeting

- Consider external audit update/strategy on proposed work.
- Consider areas in which the committee will particularly promote cooperation between the auditors, other assurance providers and review bodies.
- Review the committee's Terms of Reference.
- Consider updates on counter fraud work, whistleblowing and conflicts of interest.

## Annex F

# Key questions for an Audit and Risk Assurance Committee to ask

**This list of questions is not intended to be exhaustive or restrictive nor should it be treated as a tick list substituting for detailed consideration of the issues it raises. Rather it is intended to act as a “prompt” to help an ARAC ensure appropriate areas are considered.**

On accounting officer decision making, how do we know that:

- decisions are made to support ministers/sponsoring department with clear well-reasoned, timely and impartial advice?
- decisions are made in line with strategy, aims and objectives of the organisation set by ministers/sponsoring department and/or in legislation?
- a balanced view of the organisation’s approach to managing risk and opportunity is taken?
- only proportionate and defensible burdens on business is imposed?

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

- the risk management culture is appropriate?
- the [Orange Book](#) on risk has been reviewed and complied with?

- the board annually reviews and clearly articulates and communicates its risk appetite?
- there is a comprehensive process for identifying and evaluating risk, and for deciding what levels of risk are tolerable?
- the Risk Register is an appropriate reflection of the risks facing the organisation?
- appropriate ownership and management 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?
- is cumulative impact of risks considered?
- that the internal control framework is designed and implemented in accordance with relevant standards and best practices?
- management has an appropriate view of how effective the control environment is? How and to whom is this reported?
- will the system of control provide timely indicators of things going wrong?
- does management respond to internal control deficiencies or incidents, and are root causes and corrective actions identified and tracked?

### On risk management processes, how do we know:

- how senior management and Ministers support and promote risk management?
- how well people are equipped and supported to manage risk well?
- that there is a clear risk strategy and policy?
- that the organisation's risk appetite and tolerance have been reviewed and articulated?
- that there are effective arrangements for managing risks with partners?
- that the organisation's processes incorporate effective risk management?
- if risks are handled well, considering:

- a) key strategic risks can change very quickly?
- b) scenario planning and stress testing?
- c) 'bubbling under' risks?
  - the risk focus is wide enough:
- a) considers 'external and emerging risks'?
- b) reviews 'financial' risks and 'non-financial' risks?
  - if risk management contributes to achieving outcomes?
  - are management regularly reviewing top risks?

The [Orange Book](#) provides more detail on risk management processes, including in part 2 advice on the risk control framework including three lines of assurance.

### On the organisation's whistleblowing arrangements how do we know that:

- there are appropriate and effective whistleblowing practices in place?
- these provide suitable channels for staff and others to raise their concerns?
- the policies appropriately cover the issues on confidentiality and anonymity?
- that whistleblowers are offered appropriate support and provided with suitable and timely feedback?
- that concerns raised are dealt with properly and reported to senior management?

### On the planned activity and results of internal work, how do we know that:

- the internal audit strategy is appropriate for delivery of reasonable assurance on the whole of governance, risk management and control?
- the internal audit plan will achieve the objectives of the internal audit strategy, and in particular whether it is adequate to facilitate 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 actually 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 the latest assessment quality assessment show?
- there is appropriate co-operation between the internal and external auditors?

Internal Audit Services should periodically have an external quality assessment against the professional standards mandated for internal audit in the public sector. Results should be reported to and considered by the ARAC.

### On financial management, the accounting policies, the annual report and accounts of the organisation, do we know:

- how effective and accurate budgeting and in-year forecasting is?
- if the finance section is fit for purpose?
- does the director of finance provide relevant information, reports and advice to the committee?
- is the use of resources planned on an affordable and sustainable basis, within agreed limits?
- what the “hidden” financial risks are, relating to (inter alia):
  - a) HR?
  - b) VAT?
  - c) Overruns?
  - d) Sudden loss of funding/revenue?
- that the accounting policies in place comply with relevant requirements, particularly the Government Financial Reporting Manual?
- there has been due process in preparing the accounts and annual report and that the process is robust?

- that the annual report and accounts have been subjected to sufficient review by management and by the accounting officer and / or board?
- that when new or novel accounting issues arise, appropriate advice on accounting treatment has been gained?
- that there is an appropriate anti-fraud policy in place and that losses are suitably recorded and responded to?
- that suitable processes are in place to ensure fraud is guarded against and regularity and propriety is achieved?
- that suitable processes are in place to ensure accurate financial records are kept?
- there are effective internal controls to safeguard, channel and record resources as intended?
- that 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?
- that 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 that:

- the implementation of recommendations is monitored and followed up?
- there are suitable resolution procedures in place for cases when management reject audit recommendations, especially if management has accepted a level of risk that exceeds the organisation's risk appetite/tolerance?

### On assurances relating to the corporate governance requirements for the organisation and the annual Governance Statement how do we know that:

- corporate governance arrangements operate effectively and are clear to the whole organisation?
- the organisation has a governance structure which transmits, delegates, implements and enforces decisions?

- the accounting officer's Governance Statement correctly reflects key issues, and that robust evidence underpins it?
- the Governance Statement appropriately discloses action to deal with material problems?
- the Board 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?

Guidance on the Governance Statement can be found in Chapter three of [Managing Public Money](#).

### On the work of the ARAC itself, how do we know:

- that we are being effective in achieving our terms of reference and adding value to governance, risk management and control systems of the organisation?
- that we have an appropriate skills mix?
- that we have an appropriate level of understanding of the purpose and work of the organisation?
- that we have sufficient time to give proper consideration to our business?
- that our individual members are avoiding any conflict of interest?
- what impact we are having on the organisation?

**Annex I** of this handbook contains a self-assessment checklist that ARACs may use.

### 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?
- who ensures government expectations and standards relating to cyber security are considered and implemented within the organisation?
- does the organisation have suitably skilled and experienced staff, or access to such staff to deal with incidents?
- is there suitable awareness and ongoing training within the organisation on the risk from cyber-attack?

### On Environmental, Social and Governance (ESG) reporting how do we know that:

- ESG is effectively managed (what assurance is available)?
- are we in compliance with legal and regulatory obligations for ESG?
- what standards has the organisation adopted for ESG reporting?
- is ESG integrated with the organisation's strategies and risk management framework?
- does the organisation have a specific senior person responsible for ESG?
- are ESG targets sufficiently stretching to meet the expectations of our key stakeholders?
- how is ESG information collected and what are the data collection policies?
- what controls are in place to ensure that ESG information is reliable and complete?

### On Artificial Intelligence (AI) how do we know that:

- we are able to answer with confidence if we are using AI?

- who owns our AI strategy at Executive level?
- the strategy is aligned with our risk appetite?
- we have the appropriate expertise to oversee AI development?
- how prepared we are for new regulation?
- all relevant business areas are involved when procuring or developing AI?

# Annex G

## Competency framework

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

- understanding of the objectives of the organisation and its current significant issues and risks;
- understanding of the organisation's structure, including governance arrangements and key relationships such as that with a sponsoring department or a major partner;
- understanding of the organisation's culture;
- understanding of any relevant legislation or other rules governing the organisation; and
- broad understanding of the government environment, particularly accountability structures and current major initiatives.

The ARAC should collectively possess:

- knowledge / skills / experience (as appropriate and required) in:
  - a) accounting;
  - b) risk management;
  - c) internal / external audit; and
  - d) technical or specialist issues pertinent to the organisation's business.
- experience of managing similar sized organisations;
- understanding of the wider relevant environments in which the organisation operates; and
- detailed understanding of the government environment and accountability structures.

# Annex H

## 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.

Within GIAS, Domain III: Governing the Internal Audit Function outlines the **Essential Conditions** that must exist:

### Authorised by the ARAC

- Discuss with the HIA and senior management the appropriate authority, role, and responsibilities of the IA function.
- Discuss with the HIA and senior management other topics that should be included in the IA charter to enable an effective internal audit function.
- Review the IA charter with the HIA to consider changes affecting the organisation, such as the employment of a new HIA or changes in the type, severity, and interdependencies of risks to the organisation.
- 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.
- Authorise the appointment and removal of the HIA. (Please note that where the GIAA provides the service this would be in conjunction with the GIAA chief executive or their agent such as an operational director).
- Provide input to senior management to support the performance evaluation and remuneration of the HIA. (As above).
- Provide the HIA with opportunities to discuss significant and sensitive matters with the ARAC, including meetings without senior management present.
- Require that the HIA be positioned at a level in the organisation that enables IA services and responsibilities to be performed without interference from management. This positioning provides the organisational authority and status to bring matters directly to senior management and escalate matters to the ARAC when necessary.
- Acknowledge the actual or potential impairments to the IA function's independence when approving roles or responsibilities for the HIA that are beyond the scope of IA.
- 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.
- Approve the HIA's roles and responsibilities and identify the necessary qualifications, experience, and competencies to carry out these roles and responsibilities. (In the UK public sector qualifications are set as CCAB or IIA qualified or equivalent).

## **Overseen by the Board**

- Engage with senior management to appoint an HIA with the qualifications and competencies necessary to manage the internal audit function effectively and ensure the quality performance of internal audit services.



- 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.
- Collaborate with senior management to provide the internal audit function with sufficient resources to fulfil the internal audit mandate and achieve the internal audit plan.
- 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.
- Discuss with the HIA the quality assurance and improvement programme, (as required by the standards).
- Approve the internal audit function's performance objectives at least annually. (In the GIAA context performance objectives are set by GIAA chief executive 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; and 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 GIAA context the commissioning, management and reporting of EQA is led by GIAA chief executive).
- 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).
- Review and approve the HIA's plan for the performance of an external quality assessment. Such approval should cover, at a minimum: The scope and frequency of assessments; the competencies and independence of the external assessor or assessment team; the rationale for choosing to conduct a self-assessment with independent validation instead of an external quality assessment. (As above).
- Require receipt of the complete results of the external quality assessment or self-assessment with independent validation directly from the assessor. (As above).
- Review and approve the HIA's action plans to address identified deficiencies and opportunities for improvement, if applicable. (As above).
- Approve a timeline for completion of the action plans and monitor the HIA's progress. (As above)

# Annex I

## Audit and Risk Assurance Committee self-assessment checklist

Role and remit	YES/NO/NA	Comments/Action
1. Does the committee have written terms of reference?		
2. Are the terms of reference regularly reviewed?		
3. Do the terms of reference clearly set out the committee's role and are they consistent with the example terms of reference in this ARAC handbook?		
4. Are the terms of reference approved by the committee and the board?		
5. Are the terms of reference made publicly available?		
6. Has the committee been provided with sufficient membership, authority and resources to perform its role effectively and independently?		
7. Do committee members have appropriate authority to require reports on areas of the committee's responsibilities?		

8. Does the organisation's annual report and accounts/ Governance Statement mention the committee's existence and its broad purpose?		
Membership, induction, and training	YES/NO/NA	Comments/Action
9. Has the membership of the committee been formally agreed by the board and/or accounting officer and a quorum set?		
10. Does the committee have at least three members (or the number stated in the agreed terms of reference) who are independent and objective?		
11. Are members appointed for a fixed term?		
12. Do all members of the committee have a clear understanding of what is expected of them in their role, including: <ul style="list-style-type: none"> <li>time commitments, the duration of their appointment, training required and how this will be provided</li> <li>an understanding of the organisation – strategy, operating environment and key risks</li> <li>role of the board in managing risk and of the committee in supporting the board to provide review and challenge?</li> </ul>		
13. Have members received formal appointment letters (setting out their terms of appointment including work required) before their term of office commenced?		
14. Does the committee have the relevant/required range of skills in governance, risk, control, and financial management and is this reviewed on a regular basis?		
15. Does at least one committee member have recent and relevant financial experience?		

16. Is the committee empowered to co-opt members and procure specialist advice to support them when needed?		
17. a. Is the Chair a Non-Executive Board member (NEBM) with relevant experience to chair the committee?		
17. b. Is at least one other member a NEBM?		
17. c. Do governance processes ensure the chair of the board is not a member of the committee?		
18. Are new committee members provided with an appropriate induction, including training to help them understand the public sector accountability framework, if they have not previously worked within central government?		
19. Does the induction include a programme of engagement with the organisation to help members understand: <ul style="list-style-type: none"> <li>the organisation, its objectives, business needs, priorities, risk profile and challenges</li> <li>the organisation's vision and purpose</li> <li>the organisation's corporate governance arrangements?</li> </ul>		
20. Are regular training and development opportunities (especially for recent developments or emerging risk areas) considered and implemented for committee members?		
21. Has each member formally declared their business interests and/or conflicts of interest and have these been appropriately dealt with?		
22. Are members sufficiently independent of the other key committees of the board?		

23. Has the committee considered the arrangements for assessing the attendance and performance of each member, including the chair?		
Meetings	YES/NO/NA	Comments/Action
24. Does the committee meet regularly and at least four times a year?		
25. Do the terms of reference set out the frequency?		
26. Does the committee calendar meet the organisation's business and governance needs, as well as the requirements of the financial reporting calendar?		
27. Are members attending meetings on a regular basis and if not, is appropriate action taken?		
28. Does the accounting officer attend all meetings and, if not, are they provided with a record of discussions?		
29. Does the director of finance attend all meetings and, if not, are they provided with a record of discussions?		
30. Does the committee have the benefit of attendance of appropriate officials at its meetings, including representatives from internal audit, external audit, finance and if relevant, the sponsoring/sponsored body?		
31. Does the committee meet privately without any non-members present for all or part of a meeting if considered necessary?		

32. Do committee members or the committee chair meet separately with relevant executives as required (especially the accounting officer and any relevant newly appointed executives soon after their appointment)?		
33. a. Is a verbal or written report summarising the business taken by the committee provided to the board after each meeting?		
33. b. Does the verbal or written report offer views and advice from the committee on issues that require the board or accounting officer to take action?		
Internal control	YES/NO/NA	Comments/Action
34. Does the committee consider the findings of reviews by internal audit and others, on the effectiveness of the arrangements for governance, risk management and control?		
35. Does the committee: <ul style="list-style-type: none"> <li>• have an understanding of the overall assurances provided within the organisation (by the three lines)?</li> <li>• consider adequacy of these assurances, especially for outsourced services?</li> </ul>		
36. If the Committee does not consider the overall assurance provided to be adequate, does the committee raise these concerns to the executive to commission additional work?		
37. Does the committee consider: <ul style="list-style-type: none"> <li>• how meaningful the Governance Statement is?</li> <li>• if all pertinent issues have been included in the Governance Statement from the work the committee has undertaken during the reporting period?</li> </ul>		

38. Does the committee satisfy itself that the arrangements for governance, risk management and control have operated effectively throughout the reporting period?		
39. Has the committee undertaken deep dives into significant risks to review and challenge management's actions to manage and mitigate the risk?		
40. Has the committee considered how it should coordinate with other committees that may have responsibility for risk management and corporate governance?		
41. Has the committee satisfied itself that the organisation has adopted appropriate arrangements to counter and deal with fraud, including reporting losses, investigating fraud incidents, and submitting quarterly returns to the Cabinet Office?		
42. Does the committee receive regular reports on: <ul style="list-style-type: none"> <li>• anti-fraud policies;</li> <li>• whistleblowing processes;</li> <li>• arrangements for special investigations; and</li> <li>• relevant cases and near misses?</li> </ul>		
43. Has the committee been made aware of the role of risk management in the preparation of the internal audit plan?		
44. Does the committee's terms of reference include oversight of the risk management process to ensure risks are managed and new risks will be identified?		
45. Does the committee review the corporate risk register to ensure it reflects key strategic risks?		



46. Does the committee consider/challenge assurances provided by senior staff on the adequacy and effectiveness of control processes?		
47. Does the committee ensure any significant weaknesses found have been appropriately dealt with?		
Financial reporting and regulatory matters	YES/NO/NA	Comments/Action
48. Is the committee's role in the consideration of the annual report and accounts clearly defined?		
49. Does the committee review the annual report and accounts (including the Governance Statement) and discuss the comprehensiveness, reliability and integrity of assurances in meeting the board and accounting officer's needs?		
50. Does the committee gain an understanding of management's procedures for preparing the organisation's annual report and accounts?		
51. Does the committee consider, as appropriate: <ul style="list-style-type: none"> <li>• the suitability of accounting policies and treatments and / or changes in accounting treatment</li> <li>• assurances regarding the financial systems that produce the accounts</li> <li>• major judgements made (and if specialists were used to help with the judgements)</li> <li>• large write-offs</li> <li>• the reasonableness of accounting estimates</li> <li>• the narrative aspects of reporting</li> <li>• any differences of opinion between the auditor and executives?</li> </ul>		

52. Is a committee meeting scheduled to receive the external auditor's report to those charged with governance including a discussion of proposed adjustments to the accounts and other issues arising from the audit?		
53. Does the committee review management's letter of representation?		
54. Does the committee have a mechanism to keep it aware of topical legal and regulatory issues?		
Internal audit	YES/NO/NA	Comments/Action
55. Does the Head of Internal Audit attend meetings of the committee?		
56. Does the committee approve, annually and in detail, the annual internal audit plan (and fee) including consideration of whether the scope of internal audit work addresses the body's significant risks and does not duplicate assurances provided by other lines?		
57. Has the committee approved the internal audit mandate/formal terms of reference/internal audit charter defining internal audit's objectives, responsibilities, authority and reporting lines?		
58. Does internal audit have a direct reporting line, if required, to the committee?		
59. Has the committee considered the information it wishes to receive from internal audit?		
60. Does the committee <ul style="list-style-type: none"> <li>- receive progress reports from internal audit and review and challenge progress?</li> <li>- review the annual report from the Head of Internal Audit?</li> </ul>		

61. Are outputs from follow-up audits by internal audit monitored by the committee and does the committee consider the adequacy of implementation of recommendations?		
62. Does the committee (chair) hold private discussions with the Head of Internal Audit at least once annually?		
63. Is there appropriate co-operation between the internal and external auditors?		
64. Does the committee review <ul style="list-style-type: none"> <li>the adequacy of internal audit staffing and other resources</li> <li>internal audit performance measures</li> <li>reports on internal audit quality assurance arrangements?</li> </ul>		
External audit	YES/NO/NA	Comments/Action
65. Does the external audit representative attend meetings of the committee?		
66. Do the external auditors present and discuss their audit plans and strategy with the committee (recognising the statutory duties of external audit)?		
67. Does the committee challenge external audit plans if considered not to cover key risks?		
68. Does the committee (chair) hold periodic (at least annually) private discussions with the external auditor?		
69. Does the committee review the external auditor's annual report to those charged with governance?		

70. Does the committee ensure that executives are monitoring action taken to implement external audit recommendations?		
71. Are reports (including general value for money reports) on the work of external audit presented to the committee?		
72. Does the committee assess the performance of external audit?		
73. Does the committee consider the external audit fee and challenge it if considered inappropriate?		
Administration	YES/NO/NA	Comments/Action
74. Does the committee have a designated secretariat and is the secretariat sufficient to deal with the committee's business?		
75. Is a draft forward workplan for the committee agreed at the start of each financial year to adequately cover all areas of the committee's responsibility?		
76. Are agenda papers circulated in advance of meetings to allow adequate preparation by committee members and attendees?		
77. Do reports to the committee communicate relevant information at the right frequency, time, and in a format that is effective?		
78. Does the committee issue guidelines and/or a proforma concerning the format and content of the papers to be presented?		
79. Are minutes prepared and circulated promptly (after review by the chair) to the appropriate people?		

80. Is a report on matters arising from committee meetings presented and/or does the chair raise them at the committee's next meeting?		
81. Do action points indicate the owner and due date?		
82. Does the committee provide an effective annual report on its own activities, which is timed to support the preparation of the Governance Statement?		
Role of the Chair of the committee	YES/NO/NA	Comments/Action
83. Is the chair involved in the appointment of new committee members and the head of internal audit?		
84. Does the chair agree the annual core programme of work and agendas for each meeting?		
85. Does the chair ensure: <ul style="list-style-type: none"> <li>meetings run effectively and efficiently?</li> <li>additional meetings are convened as required?</li> <li>the number of meetings held are sufficient to allow the committee to consider all relevant areas?</li> </ul>		
86. Does the chair ensure: <ul style="list-style-type: none"> <li>committee has access to appropriate resources and support and committee budget is managed?</li> <li>Members work collaboratively?</li> <li>an effectiveness review is undertaken (or an external review is commissioned if considered relevant)?</li> <li>internal and external audit have free and confidential access if required?</li> <li>governance needs of sponsor/ALB are</li> </ul>		

considered?		
Overall	YES/NO/NA	Comments/Action
87. Does the committee effectively contribute to the overall control environment of the organisation?		
88. Are there any areas where the committee could improve upon its current level of effectiveness?		
89. Does the committee seek feedback on its performance from the board and accounting officer?		
90. Do you have any further comments?		

### **HM Treasury contacts**

This document can be downloaded from [www.gov.uk](http://www.gov.uk)

If you require this information in an alternative format or have general enquiries about HM Treasury and its work, contact:

Correspondence Team  
HM Treasury  
1 Horse Guards Road  
London  
SW1A 2HQ

Tel: 020 7270 5000

Email: [public.enquiries@hmtreasury.gov.uk](mailto:public.enquiries@hmtreasury.gov.uk)