



HM Treasury

# Audit and risk assurance committee handbook

---

March 2016





HM Treasury

# Audit and risk assurance committee handbook

---

March 2016



© Crown copyright 2016

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

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

This publication is available at [www.gov.uk/government/publications](http://www.gov.uk/government/publications)

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

PU1934

# Contents

---

		Page
Foreword		3
Chapter 1	Introduction	5
Chapter 2	Good practice principles for Audit and Risk Assurance Committees	7
Chapter 3	Membership, independence, objectivity and understanding	9
Chapter 4	Skills	11
Chapter 5	The role and scope of the Committee	13
Chapter 6	Communication and reporting	19
Annex A	The role of the Chair: good practice	21
Annex B	Committee support: good practice	23
Annex C	Model Letter of Appointment	25
Annex D	Example terms of reference	27
Annex E	Example core work programme	31
Annex F	Key questions for an audit committee to ask	33
Annex G	Competency framework	37
Annex H	Whistleblowing: guidance	39
Annex I	Cyber Security: guidance	41



# Foreword

---

Under the Corporate Governance Code in Central Government, Boards are tasked with setting the organisation's risk appetite and ensuring that the framework of governance, risk management and control is in place to manage risk within this. The Audit and Risk Assurance Committee plays a crucial role in supporting the Board to meet these obligations.

The role is a challenging one and needs strong, independent members with an appropriate range of skills and experience. It will benefit from a strong collaborative relationship with the organisation to ensure that the committee gets the support and information that it needs. The committee will also need to act as the conscience of the organisation and to provide insight and strong 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.

Whilst much of the content of this document focuses on government departments, it is equally applicable to Executive Agencies, Non-Departmental Public Bodies and other Arm's Length Bodies.



Chris Wobschall

Deputy Head of Government Internal Audit



# 1 Introduction

---

**1.1** The Treasury guidance “Corporate governance in central government departments: Code of good practice 2011” (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 chaired by a suitably experienced non executive board member (NEBM)
- an internal audit service operating to Public Sector Internal Audit Standards; and
- sponsor teams of the department’s key arm’s length bodies (ALBs)

**1.2** On Audit and Risk Assurance Committees, this principle is supported by six supporting provisions in the Code.

- the board and accounting officer should be supported by an Audit and Risk Assurance Committee
- advising on key risk is a role for the board. The Audit and Risk Assurance Committee should support the board in this role
- an Audit and Risk Assurance Committee should not have any executive responsibilities or be charged with making or endorsing any decision
- the board should ensure that there is adequate support for the Audit and Risk Assurance Committee
- the Audit and Risk Assurance Committee should lead the assessment of the annual Governance Statement for the board; and
- the terms of reference of the Audit and Risk Assurance Committee 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’ arm’s length bodies (ALBs) and non ministerial departments. Arrangements for ALBs may depend on statute. Generally, ministers do not chair ALBs, or non-ministerial departments where statute sets out the applicable governance”.

**This means that Audit and Risk Assurance Committees should be established in all departments, Executive Agencies, executive Non-Departmental Public Bodies and other ALBs.**

**1.4** Guidance to the Code suggests that the Audit and Risk Assurance Committee 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 (including areas formerly covered by the statement on internal control); and
- a risk assurance committee, with a focus on ensuring there is an adequate and effective risk management and assurance framework in place

This separation of responsibilities has historically been mainly adopted by banks and financial institutions in response to the recommendations of the Walker Review. In 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 assurance committee. Such a committee would typically focus on ensuring that the organisation is delivering its services in line with 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 in some organisations.

**1.5** The rest of this Handbook assumes that a single committee will be established (see [Annex C](#) for an example Terms of Reference).

**1.6** The Code requires that the Audit and Risk Assurance Committee should report annually on its work and how it has discharged its responsibilities in accordance with this Handbook. Any significant non-compliance with the five good practice principles of this Handbook (summarised in Chapter 2), taking account of the supporting good practice guidance, should be explained and reported in the Governance Statement. Other non-compliance may also be reported.

# Good practice principles for Audit and Risk Assurance Committees

---

This Handbook sets out five good practice principles for the Audit and Risk Assurance Committee in central government. These are summarised below and each principle is then further explained in the following chapters. Each principle is of equal importance.

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

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

## **Principle 2: Skills**

The Audit and Risk Assurance Committee should corporately own an appropriate skills mix to allow it to carry out its overall function.

## **Principle 3: The role of the Audit and Risk Assurance Committee**

The Audit and Risk Assurance Committee 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 Audit and Risk Assurance Committee work should be defined in its terms of reference, and encompass all the assurance needs of the Board and Accounting Officer. Within this, the Audit and Risk Assurance Committee should have particular engagement with the work of internal audit, risk management, the External Auditor, and financial management and reporting issues.

## **Principle 5: Communication and reporting**

The Audit and Risk Assurance Committee should ensure that it has effective communication with all key stakeholders, for example, the Board, the Group Chief Internal Auditor, Head of Internal Audit, the External Auditor, Risk Manager and other relevant assurance providers.



# Membership, independence, objectivity and understanding

***"The Audit and Risk Assurance Committee should be independent and objective; in addition each member should have a good understanding of the objectives and priorities of the organisation and of their role as an Audit and Risk Assurance Committee member."***

## Independence

**3.1** An effective Audit and Risk Assurance Committee must have members who are both independent and objective. The board and accounting officer should be supported by an Audit and Risk Assurance Committee with no executive responsibilities, comprising at least three members. 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; the committee may need to seek further independent, non-executive membership from sources other than the board in order to ensure an appropriate level of skills and experience. Cabinet Office guidance on the recruitment, appointment and development of non executive members of Civil Service boards<sup>2</sup> should still be applied. In order to operate in an independent and competent manner, the committee should possess the requisite knowledge and skills to effectively engage with and challenge the organisation (see Chapter 4).

## Relationship with the Executive

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

**3.3** The Accounting Officer and the Finance Director should routinely attend the Audit and Risk Assurance Committee. It is also normal for the Head of Internal Audit, Risk Manager (if a separate function) and a representative of the External Auditor to attend. However, the terms of reference should also provide for the Audit and Risk Assurance Committee to sit privately without any non-members present for all or part of a meeting if they so wish.

**3.4** It is also good practice for the Chair of the Audit and Risk Assurance Committee to meet with each of the Accounting Officer(s), the Finance Director, the Head of Internal Audit and the external auditor's senior representative outside of the formal committee structure (see Communication and reporting, Chapter 6). For main departments this approach should also be adopted for each of the key components of the departmental group.

## Other participants

**3.5** For some ALBs sponsored by a department there may be significant overlap or homogeneity of function, for example, covering different remits/regions, or an ALB may represent a large or

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

<sup>2</sup> "Making and Managing Public Appointments": Cabinet Office Public Appointments Unit

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 Audit and Risk Assurance Committee arrangements or to have membership crossover in the separate committees across the department, avoiding conflicts of interest. Sponsoring departments and their ALBs should ensure that the inter-relationship, including any cross-attendance of Audit and Risk Assurance Committees is agreed and appropriately documented (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 Audit and Risk Assurance Committees, in particular regarding assurance necessary to support the departmental Governance Statement.

## Conflicts of interest

**3.6** Normally the process for recording declarations of conflicts of interests in the Audit and Risk Assurance Committee 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

**3.7** All members of the Audit and Risk Assurance Committee should have a clear understanding of:

- what is expected of them in their role, including time commitments
- how their individual performance will be appraised, including a clear understanding of what would be regarded as unsatisfactory performance and the criteria which would indicate the termination of Audit and Risk Assurance Committee(s) membership should be considered
- the duration of their appointment and how often it may be renewed. Cabinet Office guidance<sup>3</sup> 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.

**3.8** The terms of appointment of an Audit and Risk Assurance Committee member should be clearly set out at the time of appointment. A model letter of Appointment is set out at [Annex B](#). The letter should also specify what other activities the individual may or may not undertake in relation to the organisation. The impact on independence of remuneration from other activities should be given careful consideration. More detailed guidance on the making of appointments can be found in "Making and Managing Public Appointments", published by the Public Appointments Unit of the Cabinet Office.

---

<sup>3</sup> "Making and Managing Public Appointments": Cabinet Office Public Appointments Unit

# 4 Skills

**"The Audit and Risk Assurance Committee should corporately own an appropriate skills mix to allow it to carry out its overall function".**

## Range of skills

**4.1** The Audit and Risk Assurance Committee 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 and control. 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.

**4.2** The Audit and Risk Assurance Committee 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 skills set should be periodically reviewed.

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

**4.4** Although Audit and Risk Assurance Committee members are recruited for their individual skills, it is vital that they are able to work collaboratively.

## Additional skills

**4.5** The Audit and Risk Assurance Committee should be empowered to both:

- co-opt 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 Audit and Risk Assurance Committee members, whatever their status or background, will have training and development needs. Those who have recently joined the Audit and Risk Assurance Committee will need induction training, to help them understand their role and/or the organisation. In particular those joining a public sector Audit and Risk Assurance Committee 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.

**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 Audit Committee members.

# The role and scope of the Committee

---

*"The Audit and Risk Assurance Committee 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."*

*"The scope of the Audit and Risk Assurance Committee's work should be defined in its Terms of Reference and should encompass all the assurance needs of the Board and Accounting Officer. Within this the Audit and Risk Assurance Committee should have particular engagement with the work of Internal Audit, the work of the External Auditor and Financial 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 and their members face is knowing whether they are giving their attention to the right issues. Key to addressing this is assurance, defined as: "an evaluated opinion, based on evidence gained from review, on the organisation's governance, risk management and internal control framework"<sup>1</sup>.

**5.2** Assurance draws attention to the aspects of risk management, governance and control that are functioning effectively and, just as importantly, the aspects which need to be given attention to improve them. An effective risk management framework and a risk-based approach to assurance helps an Accounting Officer and Board to judge whether or not its agenda is focussing on the issues that are most significant in relation to achieving the organisation's objectives and whether best use is being made of resources. The Audit and Risk Assurance Committee can help the Accounting Officer and Board to formulate their assurance needs, and then consider how well assurance received actually meets these needs by gauging 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 mechanisms at its disposal, targeting these at areas of greatest risk.

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

- the strategic outcomes and objectives which the organisation is charged to deliver, and the associated risks and control mechanisms
- the 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 risk, control and governance in accordance with the **Public Sector Internal Audit Standards**

---

<sup>1</sup> The Orange Book: Management of Risk, Principles and Concepts

**5.4** A well designed assurance framework will help. At its simplest, this will identify all the key sources of assurance in the organisation and seeks to orchestrate them to best effect. This can help to ensure that gaps are reduced or eliminated and unnecessary duplication avoided. A conceptual model that is often used to help to categorise the various sources of assurance is the ‘three lines of defence’. 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:

- first line: management assurance from “front line” or business operational areas
- second line: oversight of management activity, separate from those responsible for delivery, but not independent of the organisation’s management chain; and
- 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.

**5.5** An understanding of the three lines of defence can help the Audit and Risk Assurance Committee to play a key role in helping the Accounting Officer and Board establish an optimum mix of assurance. For example, management and oversight assurance activities can be harnessed to provide coverage of routine operations, with internal audit activity more effectively targeted at riskier or more complex areas. As well as strengthening assurance arrangements, this helps the Audit and Risk Assurance Committee to demonstrate added value to the organisation. Advice on developing assurance frameworks is available in the Treasury [Assurance Framework Guidance](#) document.

**5.6** The overall provision of assurances to the Accounting Officer and Board should be reviewed by the Audit and Risk Assurance Committee, which should constructively challenge:

- whether 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.

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

A “prompt” list of questions for Audit Committees to ask is provided at [Annex F](#).

**5.7** The overall Audit and Risk Assurance Committee view may draw attention to areas where:

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

**5.8** 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. The group should focus on assurances on cross organisational governance, risk and control arrangements to supplement Departmental or entity level assurances.

**5.9** Similarly assurance on the risk and control environment should also encompass services outsourced to external providers, including shared service arrangements, so that all key elements of the organisation are considered as parts of an "Extended Enterprise".

**5.10** It is also good practice to have reasonable oversight of risks that cross organisational boundaries, for example, in major projects. This could include a Chairs of Audit and Risk Assurance Committee Forum which meets, say, twice a year. The Group would focus on assurances on cross organisational governance, risk and control arrangements.

### **Subject Guidance**

Specific guidance for the Audit and Risk Assurance Committee on whistleblowing is provided at [Annex H](#) and on cyber security at [Annex I](#).

### **Internal and external audit**

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

**5.12** 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.

**5.13** 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 Audit and Risk Assurance Committee in discharging its responsibilities. This is because the Head of Internal Audit, in accordance with the Public Sector Internal Audit Standards, has a responsibility to provide an annual opinion on the overall adequacy and effectiveness of the organisation's governance, risk management and control processes. There is consequently a major synergy between the purpose of the Head of Internal Audit and the role of the Audit and Risk Assurance Committee.

**5.14** The role of the Audit and Risk Assurance Committee in relation to internal audit should include advising the Accounting Officer and Board on:

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

- the performance of internal audit, including conformance with the applicable standards, expected performance measures<sup>2</sup>, and the results of both internal and external<sup>3</sup> quality assurance assessments.

**5.15** Whilst the work of the External Auditor is not primarily conducted for the benefit of the organisation, the Audit and Risk Assurance Committee should nevertheless engage with this activity. As well as considering the results of external audit work and resolution of identified weaknesses, they should enquire about and consider the External Auditor's planned audit approach. They should also consider 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 unnecessary duplication of work. In addition they should review and consider the potential implications for the organisation of the wider work carried out by the external auditor, for example, Value for Money reports and good practice findings.

## Governance

**5.16** It is essential that the Audit and Risk Assurance Committee understands how governance arrangements support 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
- 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.

## Risk management and the Control Environment

**5.17** It is also essential that the Audit and Risk Assurance Committee:

- understands the organisation's business strategy, operating environment and the associated risks, taking into account all key elements of the organisation as parts of an "Extended Enterprise"
- understands the role and activities of the Board (or equivalent senior governance body) in relation to managing risk
- discusses with the Board its policies, attitude to and appetite for risk to ensure these are appropriately defined and communicated so management operates within these parameters
- understands the framework for risk assessment, management and assurance and the assignment of responsibilities
- critically challenges and reviews the risk management and assurance framework, without second guessing management, to provide assurance that the arrangements are actively working in the organisations; and

---

<sup>2</sup> See Internal Audit Performance Measures published by HM Treasury

<sup>3</sup> In accordance with the Internal Audit Quality Assessment Framework developed by HM Treasury

- critically challenges and reviews the adequacy and effectiveness of control processes in responding to risks within the organisation's governance, operations, compliance and information systems

## **Financial management and reporting**

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

**5.19** The Audit and Risk Assurance Committee will not itself be able to review the accounts in detail in order 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
- assurances about the financial systems which provide the figures for the accounts
- the quality of the control arrangements over the preparation of the accounts
- key judgements made in preparing the accounts
- any disputes arising between those preparing the accounts and the auditors; and
- reports, advice and findings from external audit (especially the Audit Completion Report – ISA 260 Report)

## **Terms of reference**

**5.20** The Audit and Risk Assurance Committee'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 Audit and Risk Assurance Committee. Model Terms of Reference for an Audit and Risk Assurance Committee are suggested at [Annex D](#).

**5.21** The responsibilities assigned to the Audit and Risk Assurance Committee should not provide any conflict with the guidance in this handbook, in particular by compromising independence. An Audit and Risk Assurance Committee should not have any executive responsibilities or be charged with making or endorsing any decisions, although it may draw attention to strengths and weaknesses in control and make suggestions for how such weaknesses might be dealt with. The overarching purpose of the Audit and Risk Assurance Committee is to advise the Board; it is then the Board that makes the relevant decisions.

**5.22** The Audit and Risk Assurance Committee 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 Audit and Risk Assurance Committee meeting; or
- providing written report(s) to the Audit and Risk Assurance Committee for the purpose of providing information to assist the committee in fulfilling its role

**5.23** The board needs adequate and timely feedback on the work of the Audit and Risk Assurance Committee in order to consider its contributions formally. A schedule of the committee's agreed delegations from the board, and the mechanisms for feedback and assurance, should be documented in the board operating framework.

**5.24** To fulfil its role, a departmental and most other organisations' Audit and Risk Assurance Committee will need to meet at least four times a year. A model "core programme" of work for an Audit and Risk Assurance Committee meeting four times a year is provided at [Annex E](#).

**5.25** The Audit and Risk Assurance Committee 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 Audit and Risk Assurance Committee

# Communication and reporting

*"The Audit and Risk Assurance Committee should ensure that it has effective communication with all key stakeholders, for example, the Board, the Group Chief Internal Auditor, Head of Internal Audit, the External Auditor, the Risk Manager and other relevant assurance providers".*

## Communication between the committee and the board

**6.1** The work of the Audit and Risk Assurance Committee needs to be effectively communicated, including across the departmental group. After each meeting of the Committee a report should be prepared for 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 (especially if the report contains advice about or to the auditors).

## Improving relationships

**6.3** It is important for the Audit and Risk Assurance Committee 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 5.10).

## Annual reports

**6.4** The Audit and Risk Assurance Committee should provide an Annual Report, timed to support the preparation of the Governance Statement. This internal report needs to be open and honest in presenting the committee's views if it is to be of real benefit to the 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 Audit and Risk Assurance Committee's work for the year past, and present the committee's opinion about:

- the effectiveness of governance, risk management and control
- the comprehensiveness of assurances in meeting the Board and Accounting Officer's needs
- the reliability and integrity of these assurances

- whether 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 Audit and Risk Assurance Committee considers pertinent to the Governance Statement and any long term issues the Committee thinks the Board and/or Accounting Officer should give attention to
- 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 Audit and Risk Assurance Committee'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 mini 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 Audit and Risk Assurance Committee, the Accounting Officer, Risk Manager (if a separate function), Head of Internal Audit and the External Auditor. Periodic discussions outside of the formal meeting help to ensure that expectations are managed and that there is mutual understanding of current risks and issues.

# The role of the Chair: good practice

---

**A.1** The role of the Chair of the Audit and Risk Assurance Committee goes beyond chairing meetings. Indeed, it is key to achieving committee effectiveness. Key activities in addition to Committee meetings should include the following.

- before each meeting the Chair and the Committee Secretary should meet to discuss and agree the business for the meeting. The Chair should take ownership of, and have final say in, the decisions about what business will be pursued at any particular meeting
- meeting time should be optimised by making sure that all agenda papers are issued in good time and then having each paper summarised outlining the key points, cross referred to the organisational business and risk agenda and stating what action the Committee is required to take
- the Chair should ensure that after each meeting appropriate reports are prepared from the Audit and Risk Assurance Committee to the Board and the Accounting Officer. An 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 NDPBs, with the Chair of the 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 Group or Departmental family environment, the Chair of the Department or Group Audit and Risk Assurance Committee should establish a mechanism enabling key stakeholders to consider the group's overall risk and assurance needs (see 5.3)
- encouraging good, open relationships between the Audit and Risk Assurance Committee, Accounting Officer, Finance Director and Internal and External auditors. There are a number of ways that a Chair can encourage this:
  - the profile of the Audit and Risk Assurance Committee can be raised to support and add weight to audit work by:
    - a promoting audit issues internally with relevant board members and other directors to make sure they appreciate 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 weeks leading up to the Committee meeting to discuss areas for the agenda and papers that should be provided; and
- arranging meetings with the internal auditors (and possibly external audit and the risk manager) immediately before the Audit and Risk Assurance Committee 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

## **5. Appraisal:**

The Chair should take the lead in ensuring that Committee members are provided with appropriate appraisal of their performance as a Committee member and that training needs are identified and addressed. The Chair should seek appraisal of his/her performance from the Accounting Officer (or Chair of the Board, as appropriate).

The Chair should ensure that there is a periodic review of the overall effectiveness of the Audit and Risk Assurance Committee and of its terms of reference.

## **6. Appointments:**

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

The Chair should also be actively involved in the appointment of the Head of Internal Audit.

# Committee support: good practice

---

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

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

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

When the Audit and Risk Assurance Committee decides to meet privately, the Chair should decide whether the secretariat members should also withdraw. If so, the Chair should ensure that an adequate note of proceedings is kept to support the Committee's conclusions and advice.



# Model Letter of Appointment

It is recommended that the following issues be included in the Letter of Appointment of an Audit and Risk Assurance Committee 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 of [organisation]. As a member of the Audit and Risk Assurance Committee 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 Audit and Risk Assurance Committee is a Committee of the Board of [organisation] and the purpose of the Audit and Risk Assurance Committee is to:

- review the comprehensiveness of assurances on governance, risk management and the control environment 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
- 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 Audit and Risk Assurance Committee's Terms of Reference is enclosed. 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 their contact details]

## Support and training

The Secretary of the Audit and Risk Assurance Committee 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 Audit and Risk Assurance Committee 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.

## Commitment and remuneration

Your duties as an Audit and Risk Assurance Committee 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].

## **Conflicts of interest**

If during your period of appointment to the Audit and Risk Assurance Committee your personal circumstances change in any way that may provide a conflict of interest for you in your Audit and Risk Assurance Committee role, you are to declare the circumstances to the Chair of the Audit and Risk Assurance Committee.

## **Appraisal**

As a member of the Audit and Risk Assurance Committee you will be subject to appraisal by the Audit and Risk Assurance Committee 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.

## **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 Audit and Risk Assurance Committee 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].

# D Example terms of reference

The Board has established an Audit and Risk Assurance Committee as a Committee of the Board to support them in their responsibilities for issues of risk, control and governance 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 Audit and Risk Assurance Committee are:

- non-executive Board members: [list those who are appointed to the Audit Committee]
- independent External members: [list those who are appointed to the Audit and Risk Assurance Committee; (in all cases indicate the date of appointment and when the appointment is due to end / become eligible for renewal)]
- the Audit and Risk Assurance Committee will be chaired by [name]
- the Audit and Risk Assurance Committee will be provided with a secretariat function by [name]

## Reporting

- the Audit and Risk Assurance Committee will formally report in writing to the Board and Accounting Officer after each meeting
- the Audit and Risk Assurance Committee will provide the Board and Accounting Officer with an Annual Report, timed to support finalisation of the accounts and the Governance Statement, summarising its conclusions from the work it has done during the year

## Responsibilities

The Audit and Risk Assurance Committee will advise the Board and Accounting Officer on:

- the strategic processes for risk, control and governance and the Governance Statement
- the accounting policies, the accounts, and the annual report of the organisation, including the process for review of the accounts prior to submission for audit, levels of error identified, and management's letter of representation to the external auditors
- the planned activity and results of both internal and external audit
- 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
- (where appropriate) proposals for tendering for either Internal or External Audit services or for purchase of non-audit services from contractors who provide audit services
- anti-fraud policies, whistle-blowing processes, and arrangements for special investigations; and
- the Audit and Risk Assurance Committee will also periodically review its own effectiveness and report the results of that review to the Board

## **Rights**

The Audit and Risk Assurance Committee 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 will have free and confidential access to the Chair of the Audit and Risk Assurance Committee.

## **Meetings**

- the Audit and Risk Assurance Committee will meet at least four times a year. The Chair of the Audit and Risk Assurance Committee may convene additional meetings, as they deem necessary
- a minimum of [number] members of the Audit and Risk Assurance Committee will be present for the meeting to be deemed quorate
- audit and Risk Assurance Committee 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 Audit and Risk Assurance Committee may ask any other officials of the organisation to attend to assist it with its discussions on any particular matter
- the Audit and Risk Assurance Committee may ask any or all of those who normally attend but who are not members to withdraw to facilitate open and frank discussion of particular matters
- the Board or the Accounting Officer may ask the Audit and Risk Assurance Committee to convene further meetings to discuss particular issues on which they want the Committee's advice

## Information requirements

For each meeting the Audit and Risk Assurance Committee will be provided (well ahead 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 from the Head of Internal Audit summarising:
  - work performed (and a comparison with work planned)
  - key issues emerging from the work of internal audit
  - management response to audit recommendations
  - changes to the agreed internal audit plan; and
  - any resourcing issues affecting the delivery of the objectives of internal audit
- a progress report (written/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 NAO, for example, Value for Money reports and good practice findings)
- management assurance reports; and
- reports on the management of major incidents, "near misses" and lessons learned.

As and when appropriate the Committee will also be provided with:

- proposals for the terms of reference of internal audit / the internal audit charter
- the internal audit strategy
- the Head of Internal Audit's Annual Opinion and Report
- quality Assurance reports on the internal audit function
- the draft accounts of the organisation
- the draft Governance Statement
- a report on any changes to accounting policies
- external Audit's management letter
- a report on any proposals to tender for audit functions
- a report on co-operation between internal and external audit; and
- the organisation's Risk Management strategy

*The above list suggests minimum requirements for the inputs which should be provided to the Audit and Risk Assurance Committee. In some cases more may be provided. For instance, it might be agreed that Audit and Risk Assurance Committee members should be provided with a copy of the report of every internal audit assignment, or with copies of management Stewardship Reports (or equivalents) if these are used in the organisation.*



# Example core work programme

---

## Spring meeting

- comment on the annual report and accounts for the year just finished prior to their finalisation and submission for audit
- consider the interim External Audit findings or update report
- advise on the content of the Governance Statement for the year just finished, to be presented alongside the finalised accounts
- review the internal audit plan for the forthcoming financial year; and
- agree the Audit and Risk Assurance Committee's annual report to the Board and Accounting Officer.

## Summer / Pre-Recess meeting

- review and consider the accounts
- consider the (emerging) External Audit opinion (Audit Completion Report) for the financial year just finished and advise the Accounting Officer on signing the accounts and Governance Statement
- consider Internal Audit's opinion for the financial year just finished; and
- discuss the implications of the result of the Accounting Officer's review of effectiveness of the system of control in relation to the Governance Statement

Some Audit and Risk Assurance Committees choose to have an additional meeting timed to deal with business other than the pre-recess finalisation of the annual report and accounts

## Autumn meeting

- consider mid-year report on emerging findings from internal audit
- consider the External Audit management letter for the previous year, any emerging findings from the current interim / in-year work of external audit, and external audit's approach to their work
- consider the external audit strategy proposed in respect of the current year's accounts; and
- consider any residual actions arising from the previous year's work of both internal and external audit

## Winter meeting

- review and challenge the internal audit strategy and the periodic work plan for the beginning of the new financial year
- consider the Audit Planning Report from External Audit

- review the overall Assurance Framework
- consider areas in which the Committee will particularly promote cooperation between auditors and other review bodies in the coming year
- re-visit emerging findings from auditors and review actions in response to the External Audit management letter; and
- consider the Committee's own effectiveness in its work

*These are all in addition to regular standing items.*

# Key questions for an audit 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 Audit and Risk Assurance Committee ensure that their work is comprehensive.

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

- the risk management culture is appropriate?
- the board has clearly articulated and communicated 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 of risk in place?
- management has an appropriate view of how effective the control environment is?
- 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?
- the system of control will provide timely indicators of things going wrong?

## 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 policies?
- 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:
  - key strategic risks can change very quickly?
  - scenario planning and stress testing?
  - ‘bubbling under’ risks?
- the risk focus is wide enough?
  - considers ‘external and emerging risks’?
  - reviews ‘financial’ risks and ‘non-financial’ risks?

- if risk management contributes to achieving outcomes?
- that management are regularly reviewing top risks?

A more detailed tool for evaluation of risk management is the “[Risk Management Assessment Framework](#)” produced by HM Treasury.

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

- the internal audit strategy is appropriate for delivery of reasonable assurance on the whole of risk, control and governance?
- 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 application of the Internal Audit Quality Assessment Framework tell us about the quality of the internal audit service?
- there is appropriate co-operation between the internal and external auditors?
- the Accounting Officer and board have taken all necessary steps to make themselves aware of any relevant information and that auditors are aware of that information?

A more detailed tool for evaluation of the quality of the Internal Audit service is the “[Internal Audit Quality Assessment Framework](#)” produced by HM Treasury.

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

- how effective and accurate budgeting and in-year forecasting is?
- the finance section is fit for purpose?
- what the “hidden” financial risks are, relating to (*inter alia*):
  - HR?
  - VAT?
  - Overruns?
  - 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 process is robust?
- that the accounts and annual report 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 accurate financial records are kept?
- that suitable processes are in place to ensure fraud is guarded against and regularity and propriety is achieved?
- 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 which the auditors stand by as being important?

**On assurances relating to the corporate governance requirements for the organisation and the annual Governance Statement<sup>1</sup>, how do we know that:**

- corporate governance arrangements operate effectively and are clear to the whole organisation?
- the AO's Governance Statement is meaningful, and that robust evidence underpins it?
- the Governance Statement appropriately discloses action to deal with material problems?
- the Board 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?

---

<sup>1</sup> Further guidance on Governance Statements is available in "Managing Public Money: Annex 3.1 and in the NAO Fact sheet: "Governance Statements: good practice observations from our audits".

- effective mechanisms are in place to ensure that assurances are reliable and adequately evidenced?
- assurances are 'positively' stated (i.e. – premised on sufficient relevant evidence to support them)?
- the assurances draw appropriate attention to material weaknesses or losses which should be addressed?
- the annual 'Governance Statement' realistically reflects the assurances on which it is premised?

**On the work of the Audit and Risk Assurance Committee itself, how do we know:**

- that we are being effective in achieving our terms of reference and adding value to corporate governance and control systems of the organisation?
- that we have the 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 an organisation?

# G Competency framework

---

All members of the Audit and Risk Assurance Committee 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 Audit and Risk Assurance Committee should corporately possess:

- knowledge / skills / experience (as appropriate and required) in:
  - accounting
  - risk management
  - internal / external audit; and
  - 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



# Whistleblowing: guidance

---

## Introduction

Whistleblowing is the process by which an individual raises a concern about a perceived past or actual issue of wrongdoing in an organisation. In the Civil Service, this includes breaches of the Civil Service Code. Whistleblowing is an important part of good government and it is essential for there to be both effective policies in place that are consistent across the Civil Service and a culture that supports whistleblowing. Employees should feel able to come forward and raise concerns without fear that they will suffer detriment or victimisation. Strong leadership and senior role modelling is essential to this.

## Background

The Public Interest Disclosure Act 1998 (PIDA), commonly referred to as whistleblowing legislation, is the employment legislation which offers protection to workers who disclose information about their employers (raising whistleblowing concerns), in certain circumstances. PIDA protects workers who ‘blow the whistle’ in the public interest i.e. disclose information about wrongdoing in their organisation, particularly if this protects customers or the wider public, in the circumstances set out in legislation.

In addition, in the Civil Service, there is also a mechanism for raising concerns under the Civil Service Code. Civil servants who believe that they are being required to act in a way which conflicts with the Code, or become aware of actions by others which they believe conflict with the Code, should report this to their line manager or someone else in their line management chain. If an individual would find this difficult, they should raise the matter with their organisation’s Nominated Officers, who have been appointed to advise staff on the Code. The independent Civil Service Commission will also consider taking complaints directly from civil servants.

All government organisations should implement or reflect all key elements of the Civil Service Employee Policy ‘Whistleblowing and Raising a Concern’ model policy and report on the effectiveness of their whistleblowing arrangements in their Annual Report and Accounts.

## Effective whistleblowing practices

The following effective whistleblowing practices are reflected in the Civil Service Employee Policy ‘Whistleblowing and Raising a Concern’ model policy. It is important that government organisations are:

- 1 Providing a clear route map to employees outlining the appropriate reporting routes for concerns.
- 2 Being clear when whistleblowing is appropriate and when other processes are better suited to resolving concerns.
- 3 Signposting to support and advice such as access to legal and counselling services.
- 4 Providing advice on confidentiality and anonymity in relation to whistleblowing.
- 5 Providing feedback to whistleblowers in a timely fashion where possible.

- 6 Investigating complaints of victimisation and putting appropriate sanctions in place for those who victimise whistleblowers.
- 7 Publicising to all employees any changes made to departmental policies and processes as a result of whistleblowing investigations, where anonymity and confidentiality allows.

## **Role of the Audit and Risk Assurance Committee**

Audit and Risk Assurance Committees (ARAC) should ensure that their organisations are operating appropriate and effective whistleblowing practices and whistleblowing should be regularly considered by the Committee.

The ARAC should confirm that a senior board member has overall responsibility for whistleblowing arrangements within the organisation. The ARAC should also confirm that HR Directors are working with their Accounting Officers to ensure that whistleblowing is regularly considered by the organisation's Board.

Consideration for the HR Directors includes:

- ensuring that effective whistleblowing practices are put in place
- accountability for ensuring these practices support the proper treatment of whistleblowers
- ensuring data is collected on the concerns raised, and examining this information to identify whether there are any lessons to be learned. This data should also be made available to the centre upon request; and
- reporting to the Board/ Accounting Officer on: the effectiveness of the organisation's whistleblowing practices, any concerns about these or systemic issues identified, and action being taken to address those issues

# Cyber Security: guidance

---

## Introduction

Cyber security is an integrated approach to preparing, protecting, detecting and responding to cyber threats; it is not just a technical issue. Cyber security refers to the technologies, processes and practices, both digital and human, designed to protect IT networks, programs and data from attack, damage, compromise or unauthorised access. It also covers the identification of and recovery from disruptions following cyber-attacks. In targeting IT systems, cyber-attacks exploit vulnerabilities in human behaviour and lack of awareness of risk.

Technological advances and the globalisation of the supply chain create opportunities for greater government efficiency and effectiveness. These include new ways to work remotely and to store and transfer data, such as mobile devices and cloud computing. As employees spend more time away from the office using a variety of IT applications and access arrangements, the dramatic increase in the flow of information in and out of the organisation becomes more difficult to control and this presents more opportunities for attackers.

Increasingly, cyber security is becoming a key issue for most boards and senior executives and non-executives are becoming more pre-emptive in evaluating cyber security risk exposure as an enterprise-wide risk management issue and not limiting it to an IT concern. Senior management will continue to play a fundamental role in understanding the risks associated with cyber security and confirming preventative and detective controls are in place.

[Ten Steps to Cyber Security](#) including its Executive Companion is the Government's primary cyber security guidance, which is designed to offer the Board practical steps to improve the protection of their networks and the information carried upon them. [Common Cyber Attacks: Reducing the Impact](#) is the evidence base which underpins much of the Government approach. There are three main aspects to ensuring cyber security:

- understanding the threat
- assessing the vulnerabilities of the organisation
- taking action and monitoring results

## Cyber threat

There are three distinct groups where principal cyber threats originate, which can be categorised as:

- 1 'attackers' – malicious hackers, criminals and 'spies' (which can include internal 'users');
- 2 'hackers' without malicious intent, who access the systems to prove that they can; and
- 3 The 'careless' users, but also poor designers and poor quality assurance which can allow the systems to leak.

Cyber threat and attacks can come in various forms:

- the most common form of cyber-attack against government is the use of **false or stolen customer credentials to commit fraud**. The uptake in online services means this form of crime can now be done on a much larger scale and foreign nationals can defraud government organisations from outside the UK.
- cyber criminals seek to **steal data from government networks that has a value on the black market**, e.g. financial information or data that can be used for ID theft. Several types of malware have been specifically designed by cyber criminals to exploit e-banking details or log-in information. Such malware is sometimes found on government networks, but financial and commercial organisations are more likely to be targeted.
- cyber criminals seek to **control computer infrastructure** and use it as a platform for carrying out other activity such as sending spam and phishing<sup>1</sup> emails. Government networks are an attractive target.
- these groups also launch **ransom attacks**, locking victims out of their data and only providing the 'key' once money is paid. Although the victims are usually members of the public and sometimes small organisations, the criminals often purport to come from a government agency leading to the potential for reputational damage.
- several of the most sophisticated and hostile foreign intelligence agencies target UK government networks to **steal sensitive information**. This could ultimately disadvantage the UK in diplomatic or trade negotiations, or militarily.
- Also, hacktivists, insiders and terrorists pose a cyber threat:
- hacktivists** crave publicity and for them, success is causing embarrassment or annoyance to the owners of high-profile websites and social media platforms that they deface or take offline. When targeted against government websites and networks, these attacks can cause reputational damage to the UK at home and abroad.
- an insider** is someone who exploits, or intends to exploit, their legitimate access to an organisation's assets for unauthorised purposes. Such activity can include unauthorised disclosure of sensitive information, facilitation of third party access to an organisation's assets, physical sabotage and electronic or IT sabotage.
- Some **terrorist** groups demonstrate an intent to conduct cyber-attacks. The sharing of expertise in online forums provides a significant opportunity for terrorists to escalate their capability.

## Role of Audit and Risk Assurance Committee

Audit and risk assurance committees' (ARAC) role is to provide assurance to the Board that the organisation is properly managing its cyber risk including appropriate risk mitigation strategies. This does not necessitate understanding the full detail of the technology involved; ARAC can confirm that the appropriate framework is in place and that continuous monitoring and improvement initiatives are adopted and sustained. It is important to understand the organisation's tolerance for risk and evaluate the risk decisions made by management. Exploring

---

<sup>1</sup> **Phishing** scams are a form of cybercrime that involves defrauding users by acting as legitimate companies or organizations in order to obtain sensitive information such as passwords and login credentials. **Spam** is the electronic equivalent of the 'junk mail'.

opportunities to share information and to use technology should be guided by the organisation's risk appetite.

In particular, to assess the organisation's cyber resilience the ARAC should evaluate whether the organisation has:

#### Governance

- controls in place to prepare for, protect from, detect and respond to cyber-attacks including management of the consequences of a cyber-security incident
- a means of monitoring the effectiveness of their cyber security controls, including where appropriate, independently testing, reviewing and assuring such controls
- identified the critical information assets which it wishes to protect against cyber-attack and who is responsible for them – whether financial data, operational data, employee data, customer data or intellectual property
- a way of identifying and agreeing the level of risk of cyber-attack that the organisation is prepared to tolerate for a given information asset; what level of cyber security risk is considered acceptable?
- an operational risk framework and internal audit plan providing cover across different areas of cyber security, not just focused on IT operations

#### Threat Intelligence; Third Party and Supply Chain

- an understanding of what data is leaving the organisation and its destination, and what associated monitoring activities are in place
- intelligence processes in place to understand the threat to the organisation's assets including a detailed understanding of which suppliers/partners connect to the organisation and how
- experienced an increase in the number of information security breaches

#### Structure and Resources

- the right skills and experience in-house to cover all relevant areas
- the right management structure in place, including the Senior Information Risk Owner (SIRO)

#### Incident Response

- an up-to-date response plan for cyber incidents which has been practiced including actions on lessons learnt

#### People, Training and Awareness

- training and development programmes to educate the workforce about cyber risks and individual responsibilities; and
- a programme of continuous improvement, or where needed, transformation, to match the changing cyber threat with appropriate performance indicators

The ARAC could consider using the organisation's SIRO to provide assurance over these and other issues by:

- getting regular briefs at ARAC meetings from the SIRO, including progress on the maturity of the organisation in information risk and cyber security

- reviewing an annual report from the SIRO as part of the financial year end assurance process, and discussing with the SIRO any issues that the ARAC should include in its recommendation for the Governance Statement

A further option for the ARAC is to consider whether one of its members could become a champion on cyber security at the ARAC (and the Board if a member), and support the SIRO.

## Related Resources<sup>2</sup>:

### Ten Steps to Cyber Security and other key guidance

Ten Steps to Cyber Security is the Government's primary cyber security guidance, which is designed to offer board rooms practical steps to improve the protection of their networks and the information carried upon them. Also to take note of, 'Common Cyber Attacks: Reducing the Impact' which is the evidence base underpinning much of the Government approach.

[www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility](http://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility)

### The Cyber Essentials Scheme

Cyber Essentials is a Government-backed and industry supported technical scheme to guide businesses in protecting themselves against cyber threats. The Cyber Essentials scheme provides businesses, large and small, with clarity on good basic cyber security practice. By focusing on basic cyber hygiene, your company will be better protected from the most common cyber threats. The Cyber Essentials badge allows your company to demonstrate that it adheres to a Government-endorsed standard. These technical essentials form part of the broader agenda described in the Ten Steps to Cyber Security guidance.

[www.cyberstreetwise.com/cyberessentials/](http://www.cyberstreetwise.com/cyberessentials/)

### Cyber Incident Response

Through a twin track approach encompassing a broadly based CREST (Council of Registered Ethical Security Testers) scheme endorsed by GCHQ and CPNI, and a small, focused GCHQ and CPNI scheme designed to respond to sophisticated, targeted attacks against networks of national significance.

[www.cesg.gov.uk/scheme/cyber-incidents](http://www.cesg.gov.uk/scheme/cyber-incidents)

### CERT UK

CERT UK is the UK National Computer Emergency Response Team. CERT UK works closely with industry, government and academia to enhance UK cyber resilience.

[www.cert.gov.uk](http://www.cert.gov.uk)

### The National Cyber Crime Unit (NCCU)

The NCCU, as part of the National Crime Agency (NCA), is the UK lead for the investigation of the most serious and organised cybercrime. The NCCU will support domestic and international

---

<sup>2</sup> Some extracted from HM Government Cyber Security: Balancing risk and reward with confidence December 2014

law enforcement, and the wider NCA, to take responsibility for tackling cyber and cyber-enabled crime affecting the UK.

The NCCU will be accessible to partners; responding dynamically to threats, providing expert advice, guidance and feedback. The NCA is not a crime reporting agency, so any reports of crime should be reported to Action Fraud (see below).

[www.nationalcrimeagency.gov.uk](http://www.nationalcrimeagency.gov.uk)

### Action Fraud

Action Fraud is the UK's single point for reporting all fraud and online financial crime. Crime can be reported online 24 hours a day, seven days a week, and the Action Fraud call centre can also be contacted to report crimes during working hours and at the weekend. When a serious threat or new type of fraud is identified, Action Fraud will place an alert on its website which contains advice for individuals and businesses to protect themselves from becoming victims of fraud.

[www.actionfraud.police.uk](http://www.actionfraud.police.uk)

**Cyber-Security Information Sharing Partnership (CISP)** The CISP facilitates the sharing of information and intelligence on cyber security threats in order to make UK businesses more secure in cyberspace. The CISP includes a secure Cyber Security: balancing risk and reward with confidence online collaboration environment where government and industry (large and SME) partners can exchange information on threats and vulnerabilities in real time.

[www.cert.gov.uk/cisp/](http://www.cert.gov.uk/cisp/)

### Centre for the Protection of National Infrastructure (CPNI)

CPNI protects national security by providing protective security advice, covering physical, personnel and cyber security, to the UK's Critical National Infrastructure (CNI). CPNI works to raise awareness at board level as well as at a technical level across the CNI. Cyber security advice and guidance is available on the CPNI website. [www.cpni.gov.uk](http://www.cpni.gov.uk)

In particular, please note **CPNI's report on insider threat:**

<https://www.cpni.gov.uk/advice/Personnel-security1/Insider-threats/>  
[https://www.cpni.gov.uk/Documents/Publications/2013/2013003-insider\\_data\\_collection\\_study.pdf](https://www.cpni.gov.uk/Documents/Publications/2013/2013003-insider_data_collection_study.pdf)

### Certified Cyber Security Consultancy

CESG announced in June 2015 the launch of its Certified Cyber Security Consultancy. This is a new approach to help Government, the wider public sector and industry get the right cyber security consultancy services to help them protect their information and to do business online with citizens safely. Certified Cyber Security Consultancy will provide a pool of consultancy services, delivered by industry companies and evaluated by CESG, to meet growing demand for high quality, tailored, expert advice.

<http://www.cesg.gov.uk/News/Pages/CESG-launches-Certified-Cyber-Security-Consultancy.aspx>  
[www.cesg.gov.uk/news/new-cesg-scheme-meets-growing-demand-cyber-security-advice](http://www.cesg.gov.uk/news/new-cesg-scheme-meets-growing-demand-cyber-security-advice)



### **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.gsi.gov.uk](mailto:public.enquiries@hmtreasury.gsi.gov.uk)