Audit and assurance policies: A guide for audit committees

KPMG Audit Committee Institute

An Audit and Assurance Policy (AAP) is intended to set out a company's approach to assuring the quality of the information it reports to shareholders (and other stakeholders) beyond that contained within the financial statements. In the following pages, we provide guidance on how a company might set the groundwork for preparing an AAP as well as what might be included.

Introduction

Regardless of any requirements to publish an AAP, boards need confidence in the robustness of their corporate reporting and wider risk management[1]. If information is important enough to report, then boards should have some assurance as to whether the information is completely and accurately captured, and transparently reported.

In some instances, assurance is required by legislation e.g., the financial statements. But in most cases it is at the companies discretion as to whether, and how much, assurance is desired. There is no one size fits all – though market forces and stakeholder expectations might drive boards' assurance choices.

Equally, not all assurance is the same. In some instances, a management self-assessment or an internal review performed by an internal audit function might provide the desired level of confidence. In other cases, the relative importance of the matter to the board, shareholders and other stakeholders, may drive the board to commission independent (external) assurance – whether reported privately to the board or subject to a public assurance opinion in line with an industry recognised assurance standard.

Even boards that have historically considered their assurance processes to be robust might find some value in taking time to pause, reflect and revisit their arrangements as they prep[are for their AAP.

[1] The UK Corporate Governance Code sets a clear expectation that boards should both present a fair, balanced and understandable assessment of the company's position and prospects; and establish procedures to manage risk and oversee the internal control framework.

Minimum contents

In 'Restoring trust in audit and corporate governance' – the Government's response to the BEIS consultation on strengthening the UK's audit, corporate reporting, and corporate governance systems – the Government confirmed its intention to require certain Public Interest Entities (PIEs) to publish an Audit and Assurance Policy every three years.

The requirement to publish an AAP will apply to public and private companies with 750 employees or more and an annual turnover of at least £750m – the so-called 750:750 PIEs.

The AAP should be published within the same section of the annual report as the audit committee report and, as a minimum, should include:

— An explanation of what independent (external) assurance, if any, the company intends to obtain in the next three years in relation to the annual report and other company disclosures beyond that required by statutory audit – for example, half-year reports, investor briefing packs, sustainability reports and website disclosures such as statements on modern slavery and gender pay gap reports.

— Specifically, an explanation of what independent (external) assurance, if any, the company plans to obtain in relation to:

  • the company's Resilience Statement in whole or part, and;

  • any reporting on its internal control framework. [Compliance with the 2018 UK Corporate Governance Code requires that board should, at least annually, carry out a review of the effectiveness of the company's risk management and internal control systems and report on that review in the annual report.]

— A description of the company's internal auditing and assurance process, including how management conclusions and judgements are challenged and verified internally; and an explanation of how the company are ensuring the integrity of their internal assurance process, and considering whether any improvements are needed in light of experience.

— A description of the company's policy in relation to the tendering of external audit services.

— An explanation of whether, and if so how, the company have taken account of shareholder and employee views in developing the AAP.

The AAP will also be required to state whether any independent (external) assurance proposed within it will be 'limited' or 'reasonable' assurance (as defined by the FRC), or whether an alternative form of engagement or review, as agreed between the company and the external provider, will be undertaken.

Additionally, the AAP will be required to state whether any independent (external) assurance – beyond the statutory audit – will be carried out according to a recognised professional standard, such as the International Standard on Assurance Engagements (ISAE) (UK) 3000 (covering assurance other than audits of historical financial information).

Companies will be free to update their AAP from year to year should they judge this necessary – for example, if issues arise that highlight or increase the value of seeking further internal or external assurance in particular areas of company reporting or activity.

Annual implementation report

In addition to the triennial AAP, the Government has confirmed its intention to require companies to publish an annual implementation report – again, within the same section of the annual report as the audit committee report – in which the directors (typically through the audit committee) provide a summary update of how the assurance activity outlined in the AAP is working in practice.

Creating an AAP

While there is some merit in publishing an AAP before the final requirements are in place, we urge boards and audit committees to favour proper consideration of their risk assessment and associated assurance needs – and produce policies that are meaningfully linked to risk and resilience – over and above the desire to be seen to be the first to adopt.

Matters for boards and audit committees to consider might include the following.

Ownership and governance arrangements

The board must be clearly accountable for the AAP whilst delegating the implementation in practical terms to the audit committee. In developing the AAP, we would expect the audit committee to work closely with the executive team and consult with the risk committee and any other oversight committees as appropriate.

Functions within the business that might be involved in the creation of an AAP might include finance, risk management, internal audit, compliance and sustainability.

Shared understanding

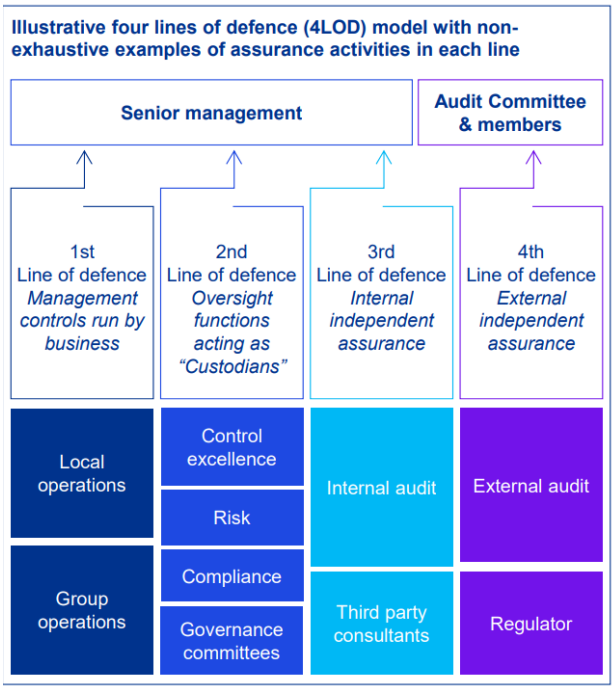
It is important that all those involved in planning and delivering the AAP have a shared understanding as to the objectives, development process, timelines, and how it will be used – as well as the sources of external reporting to which the policy will apply.

Balancing the different sources of assurance

Consider the different sources of assurance and the degree of assurance provided. What role do the four lines of defence play? Do assurance activities provide high, moderate or limited assurance? When was the assurance received? What is the role of external assurance providers verses internal assurance providers?

One way to think about the different types of assurance available to the board is the 'Four Lines of Defence' model – see below. There is some debate as to whether external audit should be described as a line of defence – nevertheless, the ICAEW includes it as such in their 2018 helpsheet.

Also, consider whether there is appropriate assurance over all the areas of interest to key stakeholders? Some areas may be immature and require preparatory work before assurance can be provided. Don't be afraid to articulate the assurance journey and when you expect to report on new areas.



Consultation with stakeholders

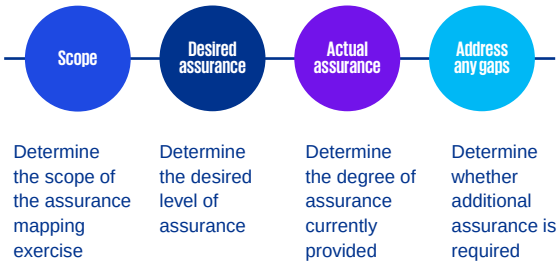
Shareholders place increasing importance on the reliability of company reporting beyond the financial statements, and employees working in critical areas of a company's business may be well-placed to advise on where any additional assurance would be helpful.

How has the company taken account of shareholder and employee views in developing the AAP? What engagement has taken place and has the stakeholder voice found its way to the board and audit committee? How can the board encourage proactive engagement with stakeholders – and meaningful input – rather than go through a tick-box exercise?

Assurance mapping

Assurance maps – which will be familiar to many audit committees – provide a visual and easy way to digest the effectiveness and completeness of a company's assurance activities. Clarity over the assurance provided by the 'four lines of defence' (see above) can also help identify any risks which require additional assurance to achieve the desired level of comfort, or any risks that are being excessively mitigated as a result of duplicated assurance activities.

A useful process to follow might be:



Determining the scope of the assurance mapping exercise

The AAP is designed to address the information a company reports to shareholders beyond that contained within the financial statements. It would be unrealistic for an assurance map to address every piece of reported information, so choices have to be made based on the materiality to shareholders and the reputation of the company. Boards and audit committees might consider:

- The principal risk and uncertainty disclosures (including any ESG risks)
- Information relating to the company's internal control framework
- Critical disclosures linked to risk and performance such as KPIs and APMs
- The Resilience Statement
- Information that is of particular interest to stakeholders or to the company's reputation such as any ESG disclosures beyond those linked to the principal risks above statements of compliance with applicable regulation
- Important information beyond the annual report including information reported in half-year reports, investor briefing packs, sustainability reports and on the company's website – such as statements on modern slavery and gender pay gap reports.

Determining the desired level of assurance

Having determined the scope of the assurance mapping exercise, the next step is to determine the desired level of assurance over each piece of reported information or the systems and processes that support such information. This is a judgement call. Every board and audit committee will have its own appetite, but in determining the desired level of assurance the board or audit committee might consider:

- The relative importance to shareholders and the reliance they may place on such information. Feedback from shareholders would be useful in this regard.
- The likelihood and potential impact of any reported risks and uncertainties – particularly the severity of any unmitigated risks.
- The magnitude of any judgements and estimates involved
- Broader stakeholder expectations and the potential reputational damage of reporting inaccurate or misleading information e.g., greenwashing
- Emerging market practice
- Any concerns relating to the underlying data and controls, including any history of misleading information or control weaknesses.

An explanation of the different levels of comfort available to the board and audit committee is set out in Appendix 1.

Ultimately, the level of comfort obtained will depend upon the rigour of the assurance framework applied, the scope of the work undertaken and the quality and experience of the assurance provider.

Determining the degree of assurance currently provided

Having determined the desired level of assurance over each piece of reported information or the systems and processes that support such information, the next stage is to benchmark the level of assurance actually received against that level.

In this stage, boards and audit committees might consider:

- The assurance provided by each level of defence and in aggregate
- The frequency and timeliness of assurance
- Whether the assurance addresses the reported information or the systems and processes that support such information
- Whether the assurance addresses the reported information (or the systems and processes) in whole or in part
- The qualifications of the assurance provider and the degree of oversight and independence (see Appendix 1)

Determining whether additional assurance is required

Having determined both the desired level of assurance and the actual assurance received, the two can be compared to assess whether:

— Additional assurance is required to achieve the desired level

— The right blend of assurance is received from across the lines of defence

— Excess assurance is being provided

If it is determined that additional assurance is required then the board and/or audit committee should consider how that is to be achieved. This may result in additional assurance being sought from an external assurance provider, or more from the first three lines of defence.

If excess assurance being provided, then there is the opportunity to create efficiencies by stripping out some assurance – though this needs to be considered holistically.

What does an assurance map look like in its most basic form

The map is intended to provide a snapshot view of the assurance obtained over an organisation's principal risks by various teams which form the organisation's four lines of defence. The below illustrative example of an assurance map captures both the gross risk scores prior to any assurance and controls and the net risk score post all assurance.

Principal Risks	Current Gross Risk score (pre controls)	First Line of Defence – Business operations "Management Controls"			Second Line of Defence – Oversight functions, e.g. Finance, Legal, HR, H&S, Risk and Compliance				Third Line of Defence – Internal Audit and other independent assurance providers		Fourth Line of Defence – Regulators and External Audit		Current Net Risk score (post controls)
		Group Function	Division	Sites	Compliance	Control Excellence	Risk	Governance Committees	Internal Audit	Third Party/ Consultant	Regulator	Ext. Audit	
1. Regulatory change	15	M	M	M	N/A	M	M	M	M	M	N/A	M	12
2. Loss of facilities	8	H	H	H	N/A	H	L	H	N	M	N/A	H	3
3. Ability to attract and retain talent	15	H	H	M	N/A	H	M	H	N	M	N	N/A	8
4. IT Resilience	8	H	M	N	M	M	O	M	N	N	H	N/A	4
5. Supply Chain incl. rising costs	9	H	H	N	N/A	H	L	M	N	N	N/A	M	6
6. ESG	12	M	M	M	M	M	M	M	N	N	N/A	N/A	8
7. Cyber	12	L	L	L	N	O	H	M	N	M	N/A	N	10
8. Transformation delivery	8	H	M	N	H	H	M	M	N	N	H	N/A	6

1 High assurance
Control(s) cover all aspects of the risk and are effective.

2 Medium assurance
Control(s) cover significant aspects of the risk and/or are partially effective.

3 Low assurance
Control(s) provide minimum coverage of the risk and/or are not effective.

4 Other assurance
Control(s) do not directly cover the risk but can be secondary source of assurance.

5 Not applicable or No assurance
N/A - Source of assurance is not applicable for this risk.
None – no assurance identified by management.

Structuring the AAP

The precise structure will necessarily reflect the nature, scale and complexity of the company. However, a good AAP should be communication focussed and seek to create an active dialogue between the company and its stakeholders. Think short and focussed!

Use plain language with well defined terms, avoid unnecessary words and complexity, use consistent terminology and work around an easy to follow structure.

One possible structure might be:

- Introduction
- Principal risks and uncertainties
- Internal controls
- Resilience Statement
- Statutory audit
- Assurance over other information in the Annual Report
- Assurance over other aspects of corporate reporting

Introduction

Explain the context for the Audit and Assurance Policy. In preparing the board and audit committee might want to consider the:

— purpose, periods covered and when it will be updated;

— process for developing, reviewing and approving the policy;

— process for seeking shareholder and other stakeholder input; and

— state of maturity and any future plans, including whether, and if so how, the company is proposing to strengthen its internal audit and assurance capabilities over the next three years

Principal risks and uncertainties

Address how the approach to assurance relates to the company's principal risks and uncertainties.

Compliance with Provision 28 of the UK Corporate Governance Code requires that the board carry out a robust assessment of the company's emerging and principal risks; and confirm in the annual report that it has completed such an assessment, including a description of its principal risks, what procedures are in place to identify emerging risks, and an explanation of how these are being managed or mitigated.

The board and audit committee might want to consider:

— How the board will determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives?

— How the board will ensure that appropriate assurance is received in respect of all the principal risks and uncertainties – including the use of any assurance mapping

— How does the board intend to rely on each of the 'four lines of defence'?

— How will new and emerging risks be identified and assessed?

Internal controls

Discuss the board's approach to assurance in relation to the system of internal controls. This should cover all material controls including financial, operational and compliance controls, including the role of internal audit.

Compliance with Provision 29 of the UK Corporate Governance Code requires that the board should monitor the company's internal control systems and, at least annually, carry out a review of its effectiveness and report on that review in the annual report.

In preparing the AAP, the board and audit committee might want to consider:

In preparing the AAP, the board and audit committee might want to consider:

— How are material internal controls defined?

— What is in scope?

— What processes will be put in place for the board's on-going monitoring of the design and operating effectiveness of material internal controls?

— Against which control framework is the effectiveness of the system of internal controls to be assessed?

— How are significant failings or weaknesses to be defined?

— What process are planned for the annual review of the effectiveness of internal controls? How will the board drawn on the results of its on-going process?

— How will the board satisfy itself that it has sound, appropriately documented, evidence to support its statement in the company's annual report and accounts?

Resilience Statement

Discuss the board's approach to assurance in relation to the new Resilience Statement (or the existing Going Concern and longer-term Viability Statements) – including the internal review approach and the extent to which the auditors have been engaged.

In preparing the AAP, the board and audit committee might want to consider:

— How has the board intends to assure itself over the robustness of the Resilience Statement?

— What, if any, external forms of assurance are planned?

— What additional assurance, if any, is to be provided by the external auditor?

Statutory audit

In preparing the AAP, the board and audit committee might want to consider:

— What approach is planned in respect of the appointment or reappointment of the external auditor – including audit tenders?

— What role will the audit committee play in negotiating the audit fee?

— How will the scope of the audit be determined (geography, risk profile, etc.) and is any additional work planned?

— What framework will be used for determining materiality?

— How will the audit committee assess the effectiveness of the audit – including the role played by management?

Assurance over other information in the Annual Report

Discuss the board's approach to determining whether the Annual Report is fair, balanced and understandable, and provides the information necessary for shareholders to assess the company's position, performance, business model and strategy.

Clarify the external auditor's responsibilities (under ISA720) in relation to the other information presented with the financial statements; and the role of internal audit.

Explain the board's approach and reasoning in determining whether any specific assurance is to be commissioned in respect of the other information included within the Annual Report – including the degree of assurance planned, the sought for independence and qualifications of any assurance provider, and the approach to be taken in respect of their appointment.

Areas for consideration might include *inter alia*:

— The Strategic Report (or aspects of it)

— Key Performance Indicators (KPIs)

— Alternative Performance Measures (APMs)

— The Directors' Fraud Statement

— The Public Interest Statement

— The Remuneration Report

— Other corporate governance statements

— ESG or Sustainability Report and/or any ESG metrics

— The Section 172(1) Statement

— The corporate culture disclosures

Where no additional assurance is planned, set out the reasons why and whether this will be reviewed in the future.

Assurance over other aspects of corporate reporting

The UK Corporate Governance Code extends the board's responsibility to present a fair, balanced and understandable assessment to interim and other price-sensitive public records and reports to regulators, as well as to information required to be presented by statutory instruments. As such, the AAP policy should also address the board's approach to assurance over *inter alia*: interim reports; gender and ethnicity pay gap disclosures; the modern slavery statement; and analyst presentations and market announcements.

Appendix 1: Different levels of comfort available to the board and audit committee

(Derived from 'Towards transparency', ICAS, 2015)

High Level Review

Oversight – The information reported to shareholders and/or the process from which it is derived will have been reviewed but not verified.

Independence –The information reported to shareholders and/or the process from which it is derived will not be subject to any independent challenge, either internally or externally.

Management verification

Oversight – The information reported to shareholders will have been subject to:

— Management established internal control procedures over the extraction and processing of the information; and

— Management scrutiny and verification.

Independence – Despite the existence of internal controls and management verification, the information reported to shareholders will not be subject to any internal or external independent oversight, or any independent external scrutiny.

Independent internal assessment

Oversight - The information reported to shareholders and/or the process from which it is derived will have been subject to internal scrutiny and review.

Independence – This assessment is likely to have been performed by internal specialist functions, including internal auditors, who are independent of those responsible for the production of the KPI.

Reporting – The information reported to shareholders and/or the process from which it is derived may be the subject of an internal report.

Independent external assessment (private report)

Oversight - Here, The information reported to shareholders and/or the process from which it is derived will have been subject to external scrutiny and challenge, the extent of which will have been agreed in advance between the external third party assurance provider and the company.

Independence – The external scrutiny and challenge will have been undertaken by an external party, independent of the company.

Reporting - A report is made only to the company (board, audit committee or senior management) but no opinion is expressed publicly.

Independent external assessment (public report)

Oversight - The information reported to shareholders and/or the process from which it is derived will have been subject to external scrutiny and challenge. This may be the subject of a separate engagement from the financial statements audit.

Independence - The external scrutiny and challenge will have been undertaken by an external party, independent of the company.

Reporting – The outcome will be a report in which an opinion or conclusion is provided to third parties/publicly. Note that the AAP will be required to state whether any independent assurance proposed within it will be 'limited' or 'reasonable' assurance (as defined by the FRC), or whether an alternative form of engagement or review, as agreed between the company and the external provider, will be undertaken.

— Limited Assurance – this level of assurance is lower than that of a financial statements' audit but still provides the user with some level of comfort over the integrity of the information. The nature, timing and extent of procedures performed in a limited assurance engagement is limited compared with that necessary in a reasonable assurance engagement, but is planned to obtain a level of assurance that is, in the practitioner's professional judgment, meaningful (ie clearly more than inconsequential).

— Reasonable Assurance – this level of assurance is equivalent to that provided in a financial statements' audit engagement and is greater than Limited Assurance.

Additionally, the AAP will be required to state whether any independent assurance – beyond the statutory audit – will be carried out according to a recognised professional standard, such as the International Standard on Assurance Engagements (ISAE) (UK) 3000 (covering assurance other than audits of historical financial information).

The KPMG Board Leadership Centre

The KPMG Board Leadership Centre offers support and guidance to non-executive directors, whether managing a portfolio non-executive career or embarking on a first appointment. Membership offers you a place within a community of board-level peers with access to topical and relevant seminars, invaluable resources and thought leadership, as well as lively and engaging networking opportunities. We equip you with the tools you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business.

Learn more at www.kpmg.com/uk/blc.

Contact us

Timothy Copnell
Board Leadership Centre
T: +44 (0)20 7694 8082
E: tim.copnell@kpmg.co.uk

www.kpmg.com/uk/blc