

Overall aim of the Audit and Assurance Policy

The Government Response states that the primary purpose of the AAP is to require companies to demonstrate to their stakeholders how they are assuring information beyond the financial statements, whether internally or externally, and how they are considering where any additional internal or external assurance may be needed going forward.

Background

In his review into the quality and effectiveness of audit, Sir Donald Brydon recommended that directors present a three-year rolling AAP to shareholders in order "to help frame the role of the auditor(s) and to make clearer the extent of all assurance in regard to the information they [as directors] communicate".

The BEIS White Paper proposed that public interest entities should publish an AAP which sets out a company's approach to assuring the quality of the information it reports to shareholders beyond that contained in the financial statements. The White Paper invited views on whether the AAP should be published annually or every three years, and whether it should be subject to an advisory shareholder vote. On the basis that, going forward, reported information will include the new Resilience Statement (closely linked to principal and emerging risks) and an internal controls attestation, we believe there is value in starting the AAP with consideration of how risk and internal controls are managed within the business and the level of assurance obtained over those processes as well as assurance over reported information.

The AAP is intended to cover both internal and external sources of assurance and to encompass assurance beyond that required for the financial statements (see Appendix A for further discussion on types of assurance). There is recognition that assurance will develop over time; some companies may believe that certain aspects of their corporate reporting, ESG metrics for example, are relatively immature in their development, and directors may therefore feel that they are not yet ready to be subject to formal assurance. In these cases, walkthroughs by internal or external auditors will have benefit in identifying areas for improvement so that assurance can be achieved over time.

Most companies will have a combined audit and risk committee; but others, particularly in regulated industry sectors, will have a separate risk committee. The AAP should acknowledge which model is followed, but is intended to be a unifying document encompassing both models.

Matters to consider when setting your first Audit & Assurance Policy

Developing the policy – to be developed by the audit committee, in consultation with the executive committee, and approved by the board. It will be useful to seek the input of internal and external auditors. Consider the remits of both the risk committee and the audit committee as well as the sustainability committee, and any other committees whose work finds its way into the Annual Report.

Assurance readiness – consider how best to build up assurance, recognising that some areas may currently be immature and may require preparation before assurance can be provided.

Consultation process – how will you seek to engage with your shareholders, employees and other key stakeholders? Will you also seek input on the risk section of your annual report?

Materiality – on what basis will you determine the materiality of particular aspects of reporting? Recognising that the measurement and relevant considerations will differ depending on the nature of the reporting.

Transparency – the Government has confirmed that, for PIEs that are required to produce an audit committee report, the triennial AAP and the annual implementation report should be published within the same section of the annual report as the audit committee report. How will it align to the Audit Committee Report and other annual report disclosures around risk management frameworks?

Update – what mechanism will you use to update the policy to reflect any changes in the business model, strategy and/or risks and to evidence learning?

AGM – how will you use the AGM to communicate the policy to shareholders and other stakeholders? Will the Audit Committee Chair be available to answer questions in relation to the policy?

Possible structure of the Audit & Assurance Policy

Introduction

Explain the context for the policy and the governance around it

- Describe the aim of the Audit & Assurance Policy
- Describe the process for developing it: who has taken ownership, the approval and review process and any stakeholder engagement which has taken place
- Confirm the time period for which the policy is intended to apply and when/how updates will be undertaken
- Recognise that the policy will evolve over time in response to regulatory demands, stakeholder dialogue and the maturing of processes. If the company is adopting a staged approach to assurance over elements of the front half, it would be worth stating this
- Where there is a separate risk committee, the company may choose to explain here the role and remit of that committee and possibly also describe how activities are coordinated with the audit committee to achieve the aim of the AAP if not covered in sufficient detail in the committee mandates or in the annual report

PART 1 - Assurance around the handling of risk and internal controls

A reminder of the Code requirement

UK Corporate Governance Code Principle C

The board should establish a framework of prudent and effective controls, which enable risk to be assessed and managed.

UK Corporate Governance Code Principle O

The board should establish procedures to manage risk, oversee the internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives.

UK Corporate Governance Code Provision 29

The board should monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness and report on that review in the annual report. The monitoring and review should cover all material controls, including financial, operational and compliance controls.

UK Corporate Governance Code Provision 25

The audit committee's roles and responsibilities include:

- Reviewing the company's internal financial controls and internal control and risk management systems, unless expressly addressed by a separate board risk committee composed of independent non-executive directors, or by the board itself
- Monitoring and reviewing the effectiveness of the company's internal audit function or, where there is not one, considering annually whether there is a need for one and making a recommendation to the board

a) Explain how the company's approach to assurance relates to the Risk Report

- The 'Risk Report' refers to the Principal Risks and Uncertainties section of the annual report addressing the requirement of Provision 29 of the UK Corporate Governance Code for boards to carry out a robust assessment of the risks facing the company (also important to remember that DTR4.2.7(2) calls for the half-yearly financial report to include a description of the principal risks and uncertainties for the remaining six months of the financial year and to consider the alignment between this and the 'Risk Report').
- Explain how the three lines of defence model operates within the company.
- Explain what mechanism has been used to identify any gaps where current audit and assurance does not cover the risks identified in the Risk Report, e.g. an assurance map.
- Explain how new areas of risk are considered - such as those arising from new businesses, or new geographies, from technology, from changes to strategy and business model, from changes in critical third parties such as outsourced providers, from changes to reporting requirements and from external factors such as climate change.

- b) Explain the approach to compiling the Resilience Statement (or now, the Going Concern and Viability Statement), the internal review approach and the extent of auditor engagement. The AAP will be required to set out whether, and if so how, a company intends to seek independent (external) assurance over any part of the Resilience Statement.
- Describe the approach to the resilience statement – short, medium and long term.
 - Describe the way that supporting analysis is produced, scenarios tested, assumptions or qualifications.
 - Explain the involvement of the external auditor and/or any other assurance over the process.

For information – Government Response Section 3.1 – the Resilience Statement

- companies to report on matters that they consider a material challenge to resilience over the short and medium term, together with an explanation of how they have arrived at this judgement of materiality
- in doing so, companies will be required to have regard to the following:
 - any materially significant financial liabilities or expected refinancing needs occurring during the assessment period of the short and medium term sections of the Resilience Statement;
 - the company's operational and financial preparedness for a significant and prolonged disruption to its normal business trading;
 - significant accounting judgements or estimates contained in the company's latest financial statements that are material to the future solvency of the company;
 - the company's ability to manage digital security risks, including cyber security threats and the risk of significant breaches of its data protection obligations;
 - the sustainability of the company's dividend policy;
 - any significant areas of business dependency with regard to the company's suppliers, customers, products, contracts, services or markets which may constitute a material risk; and
 - the impact on the company's business model of climate change, to the extent that this is not already addressed by the company in other statutory reporting.
- companies to choose and explain the length of the assessment period for the medium-term section and to include a description of how resilience planning over the chosen period aligns with the company's strategy and business investment cycle
- the disclosure must make clear how the company's assumptions on resilience planning and risk management are influenced by and relate to its strategy on the one hand, and also the main trends and factors that are likely to affect the future development, performance and position of the company's business
- companies to perform at least one reverse stress test
- companies to identify any material uncertainties to going concern, that existed prior to the taking of mitigating action or the use of significant judgement, which the directors consider are necessary for shareholders and other users of the statement to understand the current position and prospects of the business

- c) Explain the approach taken to obtaining and reporting on assurance around internal controls, in relation to financial reporting, as well as operational and compliance controls
- Explain the activities undertaken to document the system of internal control, including how material controls have been defined (see flowchart at Appendix B in relation to internal controls over financial reporting)
 - Explain the process for monitoring the design and operating effectiveness of material controls (this should identify the framework against which the evaluation of controls is undertaken (e.g. COSO), which internal function and/or external provider undertakes an evaluation (if any) and to whom are the results of the evaluation are reported). If none currently, explain when it is planned and the steps required for getting to that point
 - Set out the criteria against which the board evaluates whether an operational process is either in or out of scope for monitoring and review and who concludes on this
 - Explain the annual process for reviewing effectiveness of internal controls for those agreed to be in scope
 - Explain the agreed definition of a significant control failure or weakness that would require detailed consideration and disclosure of remediating actions
 - Explain how the disclosures on internal control in the annual report are prepared and reviewed
 - Review the explanations given above to ensure they provide reasons the procedures described are effective

For information – Government Response Section 2.1 – Stronger internal company controls

The Government is asking the FRC to strengthen the internal control provisions in the UK Corporate Governance Code to provide for an explicit statement from the board about their view of the effectiveness of the internal control systems (financial, operational and compliance systems) and the basis for that assessment.

The AAP must state whether or not there are plans to seek external assurance of the company's reporting on internal controls.

PART 2 – Assurance over company reporting

A reminder of the Code requirements

UK Corporate Governance Code Principle M

The board should establish formal and transparent policies and procedures to ensure the independence and effectiveness of internal and external audit functions and satisfy itself on the integrity of financial and narrative statements².

UK Corporate Governance Code Principle N

The board should present a fair, balanced and understandable assessment of the company's position and prospects.

UK Corporate Governance Code Provision 25

The audit committee's roles and responsibilities include:

- Monitoring the integrity of the financial statements of the company and any formal announcements relating to the company's financial performance, and reviewing significant financial reporting judgements contained in them
- Providing advice (where requested by the board) on whether the annual report and accounts, taken as a whole, is fair, balanced and understandable, and provides the information necessary for shareholders to assess the company's position and performance, business model and strategy
- Conducting the tender process and making recommendations to the board, about the appointment, reappointment and removal of the external auditor, and approving the remuneration and terms of engagement of the external auditor
- Reviewing and monitoring the external auditor's independence and objectivity
- Reviewing the effectiveness of the external audit process, taking into consideration relevant UK professional and regulatory requirements

² The board's responsibility to present a fair, balanced and understandable assessment extends to interim and other price-sensitive public records and reports to regulators, as well as to information required to be presented by statutory instruments.

External audit services

- Describe the policies and process for appointing the external auditors and the timeline of their tenure
- Explain how the scope of the audit is determined (for example, geography and risk profile of components/subsidiaries)
- Explain the fee basis for external audit work
- Explain the policy for the provision, by the external auditor, of non-audit services
- Describe the framework for decisions about materiality
- Indicate how shareholders should interpret the resulting audit reports
- Explain how the audit committee plans to monitor audit quality
- Make clear the external auditor's responsibilities in relation to other information presented with the financial statements so that there is no misunderstanding or expectation gap. As a reminder the auditor is required (under ISA720) to consider whether there are any material inconsistencies between the other information and the financial statements, the auditor's knowledge obtained in the audit or the auditor's understanding of the legal and regulatory requirements applicable to the statutory other information.

Independent assurance

Explain the board's approach to determining what other information to assure, to what level of assurance. Where no assurance is provided, it would be informative to communicate the reasons and whether this might be reviewed in the future. The AAP will be required to state whether any independent assurance proposed within it will be 'limited' or 'reasonable' assurance (see Appendix A for further discussion on types of assurance) or whether an alternative form of engagement or review, as agreed between the company and the external provider, will be undertaken. In addition, 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. For example:

Narrative reporting – Consider making reference to the requirement for the annual report to contain sufficient information for an understanding of the company's business model, strategy and performance and that the annual report, taken as a whole, is fair, balanced and understandable, and describe the review/assurance process over the narrative sections of the annual report.

Key performance indicators – including any Alternative Performance Measures – as these are the key metrics used by management to demonstrate performance and delivery of the strategy, the board ensures that these metrics are subject to [external assurance/ evaluation by internal audit in accordance with a plan agreed with the audit committee] prior to approval of the strategic report each year.

ESG metrics (including those in relation to climate change and metrics used in the Section 172 statement) – given the increased focus by our investors and wider stakeholders on these metrics and the lack of consistent standards for measurement, the board requests that these metrics are subject to [external assurance/ evaluation by internal audit in accordance with a plan agreed with the audit committee] prior to approval of the strategic report each year.

Remuneration Report disclosures – some elements of the Remuneration Report are required by law to be subject to external audit and those elements are clearly identified in the report, other disclosures in the report are subject to [evaluation by internal audit in accordance with a plan agreed with the audit committee] prior to approval.

Culture – as a board we are continuing to evolve our approach to monitoring and assessing culture and to develop the range of metrics necessary to provide a multi-dimensional view of the culture within our organisation. In order to ensure that these metrics and our disclosure of relevant activities have integrity, the board asks internal audit to undertake an evaluation of the metrics and disclosures

prior to approval.

Section 172(1) Statement – describe the board oversight process and to what extent the disclosure within the statement has been subject to any form of assurance.

Assurance over the half-yearly report

- Explain the board's decision on assurance over the half-yearly report. Has the external auditor been asked to provide an audit report or review report (see Appendix A for further detail) or is no external assurance provided? In the absence of any external assurance what internal assurance processes are undertaken in relation to the half-yearly report?

Assurance over other reporting by the company

- As noted above, the UK Corporate Governance Code also places responsibility on the board to present a fair, balanced and understandable assessment extends beyond the annual and half-yearly reports to other price-sensitive public records and reports to regulators, as well as to information required to be presented by statutory instruments. This would include reporting such as the Modern Slavery Statement, Gender Pay Gap, the Ethnicity Pay Gap and Payment Practices. It would also include presentations to analysts, market announcements and other regulatory reporting.
- The board should explain the approach to assurance over each of these important areas of corporate reporting which, by their nature, do not fall within the annual report assurance process but could have significant market and reputational impacts if not done with integrity.

Internal audit and assurance processes

- Describe the company's internal audit and assurance processes including to what extent management conclusions and judgements in the annual report and accounts are challenged and verified internally.
- To the extent that any items of the reporting matters noted above are subject to internal assurance, explain how the company is proposing to strengthen its internal audit and assurance capabilities to undertake this work.

PART 3 – Stakeholder engagement

- Explain whether, and if so how, shareholder and employee views have been taken into account in the formulation of the AAP.

PART 4 – The Assurance Budget

- Neither the White Paper or the Governance Response include consideration of budget or costs for audit and assurance (as the Brydon recommendation did) but this could be useful information for stakeholders and companies should decide if they wish to make it public or not. Set out the company's budget for assurance divided by broad categories of expenditure planned for the first year of the rolling three-year period covered:
 - External fees
 - The cost of internal audit
 - Other forms of assurance that the company chooses to obtain

APPENDIX A

TYPES OF ASSURANCE

Internal assurance – the “three lines of defence”

First line – represented by day-to-day risk management and control, likely to be within business units, including operational and technology aspects.

Second line – operate with a level of independence from day-to-day risk management and control (the first line) to oversee risks. They develop and maintain risk management policies, frameworks and approaches, identify and monitor risks, and report to senior management.

Third line – usually an internal audit function providing independent assurance to the board that the first and second lines of defence are working appropriately.

External assurance engagements

Reasonable assurance engagement — an assurance engagement in which the provider reduces engagement risk to an acceptably low level in the circumstances of the engagement as the basis for the conclusion. The conclusion is expressed in a form that conveys the provider's opinion on the outcome of the measurement or evaluation of the underlying subject matter against certain criteria.

Limited assurance engagement — an assurance engagement in which the provider reduces engagement risk to a level that is acceptable in the circumstances of the engagement but where that risk is greater than for a reasonable assurance engagement. The provider expresses a conclusion in a form that conveys whether, based on the procedures performed and evidence obtained, a matter(s) has come to the provider's attention to cause them to believe the subject matter information is materially misstated. 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 provider's professional judgment, meaningful.

In addition, an assurance engagement can be either an attestation engagement or a direct engagement:

- An attestation engagement will usually involve a provider being asked to affirm an assertion made by somebody else
- A direct engagement is where the provider measures or evaluates the underlying subject matter against the applicable criteria and presents the resulting subject matter information as part of, or accompanying, the assurance report

Half-yearly reports – the difference between an audit report and a review report

A review, in contrast to an audit, is not designed to obtain reasonable assurance that the half-yearly report is free from material misstatement. A review consists of making inquiries, primarily of persons responsible for financial and accounting matters, and applying analytical and other review procedures. A review may bring significant matters affecting the half-yearly report to the auditor's attention, but it does not provide all of the evidence that would be required in an audit.

APPENDIX B

A framework for developing and reviewing internal controls over financial reporting

STEP 1 – initial assessments and entity level controls

- Start with a detailed understanding of the business model
- Undertake a financial risk assessment and fraud risk assessment
- Establish clear and robust entity level controls to ensure the right “tone from the top”
- Define a hierarchy of delegated authorities from the board

STEP 2 – confirmation of in scope systems and identification of material controls

- Obtain clarity over in scope systems and related general IT controls
- Generate robust process documentation for material business cycles, with clear process owners
- Identify the material controls

STEP 3 – establish robust monitoring and review processes

- Define and evidence a robust process for on-going monitoring of the design and operating effectiveness of material controls
- Define and evidence a robust process for a year-end assessment of the design and operating effectiveness of material controls

STEP 4 – establish clear reporting protocols and accountability for action

- Define a significant control failure or weakness that would require detailed consideration and disclosure of remediating actions
- Define reporting processes including remedial action tracking



This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2022 Deloitte LLP. All rights reserved.

Designed by CoRe Creative Services. RITM1102405