Deloitte.

The Deloitte Academy
June 2021

Developing your company's Audit & Assurance Policy

Updated for the BEIS White Paper proposals

Introduction

The concept that a public company should establish an Audit and Assurance Policy ("AAP") and publish it for shareholder consultation was first introduced by the Brydon Review in December 2019. The intention was that the AAP would be part of the architecture of activities which should provide "confidence in a company, in its directors and in the information for which they have responsibility to report, including the financial statements". Brydon positioned the recommendation as an important part in boards communicating the "deserved confidence" in their company's reporting.

In its 18 March 2021 White Paper 'Restoring trust in audit and corporate governance', the Government stated that it agreed with the Brydon Review recommendation and proposed to introduce a statutory requirement on public interest entities to publish an AAP annually that describes the company's approach to seeking assurance of its reporting information over the next three years. In the case of listed entities, the proposal is that the AAP would be subject to an advisory shareholder vote.

The AAP concept neatly addresses a number of issues together: First, in publishing the policy the directors convey to readers the extent of assurance over the information they communicate; second, the policy helps frame the role of the auditor beyond that required for the financial statements, injecting much needed clarity in that area; and, finally, it facilitates dialogue between the company and shareholders and other stakeholders. Overall, the policy will describe more clearly to users "the extent to which the annual report and other disclosures have been scrutinised, whether by the existing company auditor or someone else". In developing their policy, boards will consider the areas where assurance is required, and who should be the provider - the external auditor, the internal audit function or perhaps other third parties providing assurance, taking into account factors such as credibility, independence and competence.

We believe that leading audit committees will not wait until the AAP becomes mandatory. Leading audit committees will recognise that developing such a policy will be worthwhile in itself. In addition, we encourage audit committees to go beyond the White Paper proposal to broaden the coverage of the policy to include both:

- the directors' approach to obtaining assurance over the range of reporting for which they have responsibility; and
- the assurance processes around the handling of risk and internal controls (which aligns with another White Paper proposal for a board attestation on internal controls over financial reporting).

We are aware that some companies do intend to publish their AAP for consultation with shareholders, whereas others are choosing to keep it private for now. To help companies who wish to develop their policy, we offer in this guide a possible structure with considerations and supporting commentary. We hope this contribution is useful and would be very pleased to hear from directors as they develop their thinking for reflection in future editions.

Overall aim of the Audit and Assurance Policy

The aim of the AAP is to provide a proportionate and flexible means for companies to explain whether, and if so how, they are obtaining assurance on any company reporting beyond that which is required by the annual company audit.

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 publication of the AAP allows the directors to invite shareholders to express views on the company's approach to audit and assurance in an advisory vote.

It is interesting to note that whilst the Brydon recommendation specifically referenced that the AAP should cover assurance over both the integrity of reporting and the handling of risk, the White Paper proposal for an AAP has focused on assurance over reported information only. 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.

See Appendix C for relevant extracts from the BEIS White Paper.

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 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 – where will you publish it? Website/annual 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 annually 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. Provide enough information to enable shareholders to "judge the extent to which a company's Audit and Assurance Policy enables satisfactory assurance over the Resilience Statement as a whole".

- Describe the three stage 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 – BEIS White Paper Section 3.1 - the Resilience Statement

- short-term section of the Statement would incorporate companies' existing going concern statement, including disclosure of any material uncertainties considered by management during their going concern assessment, which were subsequently determined not to be material after the use of significant judgement and/or the introduction of mitigating action
- medium term section of the Statement would incorporate the existing viability statement requirements, the Government proposes a mandatory assessment period of five years, rather than the three year period currently chosen by most companies who produce viability statements
- companies should include at least two reverse stress testing scenarios
- specific disclosures suggested for both the short and medium-term sections might include:
  - threats to liquidity, solvency and business continuity in response to a major disruptive event (such as a pandemic) which disrupts normal trading conditions;
  - supply chain resilience and any other areas of significant business dependency (e.g. on particular markets, products or services);
  - digital security risks (including both external cyber security threats, and the risk of major data breaches arising from internal lapses);
  - the business investment needs of the company to remain productive and viable;
  - the sustainability of the company's dividend and wider distribution policy; and
  - climate change risk.
- the content of the long-term section will not be prescribed but should set out what the directors of the company consider to be the main long-term challenges to the company and its business model, and how these are being addressed

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 – BEIS White Paper Section 2.1 – Directors' accountability for internal controls

Government's initial preferred option:

- Directors should be required to:
  - carry out an annual review of the effectiveness of the company's **internal controls over financial reporting;**
  - explain – as part of the annual report and accounts - the **outcome** of the annual review, and make a statement as to whether they consider the systems to have **operated effectively;**
  - disclose the **benchmark system** that has been used to make the assessment; and
  - explain how they have **assured themselves** that it is appropriate to make the statement.
- **Deficiencies** identified should be disclosed with a remedial action plan including timeframe
- Whether the statement should be subject to **external audit and assurance** should usually be a matter for audit committees and shareholders as part of the Audit & Assurance Policy

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 statements[1].

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

[1] 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) and any specific areas of focus which the board/audit committee/shareholders[2] have requested
- 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[3]
- 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. 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.

[2] Further to a recommendation by Sir Donald Brydon, the BEIS White Paper is proposing that a formal mechanism should be established to enable audit committees to gather shareholder views on the audit plan having had access to the board's latest statement on the company's emerging and principal risks.

[3] Further to a recommendation from the CMA, the BEIS White Paper is proposing to impose additional requirements on audit committees in relation to the appointment and oversight of auditors. Assuming this is adopted audit committees will be required to submit regular reports to the regulator on how they are meeting these responsibilities.

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

- The White Paper does not incorporate the 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:

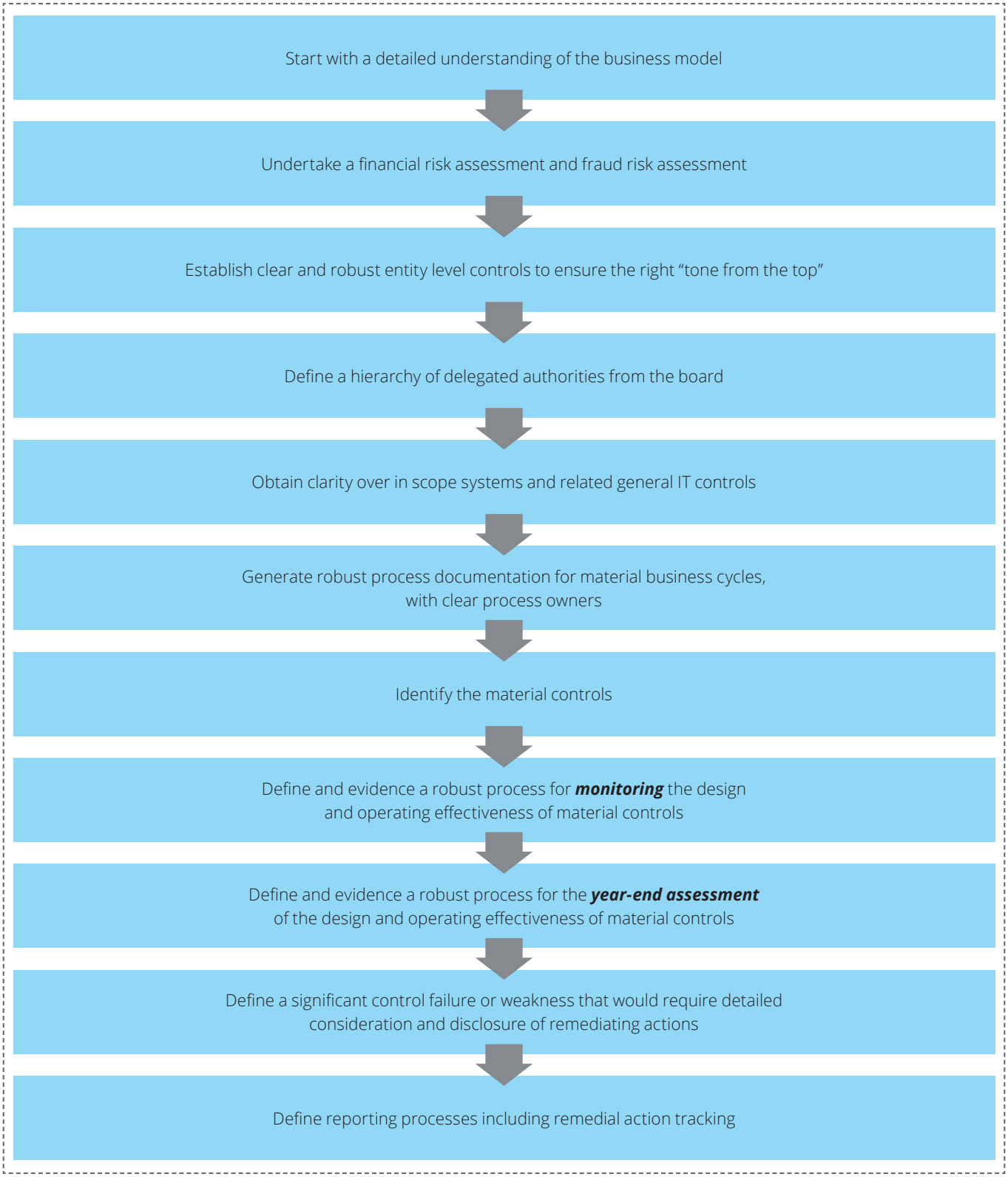
- An attestation engagement will usually involve a provider being asked to affirm an assertion made by somebody else
- A direct engagement is where the provider measures or evaluates the underlying subject matter against the applicable criteria and presents the resulting subject matter information as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



APPENDIX C

Relevant extracts from the BEIS White Paper – March 2021

Required content of the Audit and Assurance Policy (Section 3.2)

3.2.9 Taking into account suggestions by the Brydon Review regarding the content of the Audit and Assurance Policy, and existing reporting requirements on company auditors and audit committees, the Government invites views on whether the Policy should include the following new disclosures at a minimum:

- An explanation of what independent assurance, if any, the company intends to obtain in the next three years in relation to the annual report and other company disclosures beyond required by statutory audit. The Government proposes that this should include an explanation of what independent assurance, if any, the company plans to obtain in relation to:
  - the company's Resilience Statement in whole or part, and other disclosures related to risk
  - the effectiveness of the company's internal controls framework.
- A description of the company's internal auditing and assurance processes. This might include how management conclusions and judgements in the annual report and accounts can be challenged and verified internally, and whether, and if so how, the company is proposing to strengthen its internal audit and assurance capabilities over the next three years.
- A description of what policies the company may have in relation to the tendering of external audit services (for example, whether the company is prepared to allow the external company auditor to provide permitted non-audit services).
- An explanation of whether, and if so how, shareholder and employee views have been taken into account in the formulation of the Audit and Assurance Policy.

3.2.10 The Government is proposing that risk and viability reporting, and the effectiveness of a company's internal control framework, should be routinely considered for possible additional assurance as part of the formulation of every new Audit and Assurance Policy, since the consequences of inadequate reporting or processes in these areas could be particularly significant for the future of the company.

3.2.11 The Brydon Review also made recommendations in relation to the audit of Alternative Performance Measures (APMs) and Key Performance Indicators (KPIs), and company statements covering how directors have complied with their duty under Section 172 of the Companies Act to have regard to certain stakeholder interests and other matters. For reasons set out separately in this document, the Government is not minded to require the statutory audit to cover these matters, but has invited views on how possible additional assurance on APMs/KPIs and the Section 172 statement might be considered through the Audit and Assurance Policy.

Deloitte.

Designed by CoRe Creative Services. RITM0727139