Deloitte.

The Deloitte Academy
November 2020

Developing your company's Audit and Assurance Policy

Introduction

The concept that a public company should establish an Audit and Assurance Policy and publish it for shareholder consultation was introduced by the Brydon Review. The Audit and Assurance Policy is 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". The recommendation is an important part in boards communicating the "deserved confidence" in their company's reporting.

The 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 would help frame the role of the auditor beyond that required for the financial statements, injecting much needed clarity in that area; and, finally, it would facilitate dialogue between shareholders and other stakeholders with the company. Overall, the policy will describe "what processes have been considered [by the board] and reasons for their confidence in their effectiveness". 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 introduction of an Audit and Assurance Policy becomes mandatory. Leading audit committees will recognise that developing such a policy will be worthwhile in itself, stimulating thinking in two areas:

- 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.

We are aware that some companies do intend to publish their Audit and Assurance Policy for consultation with shareholders; others may choose 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 Audit and Assurance Policy is to provide greater clarity and visibility of how, and to what extent, directors "**are assuring the integrity of reporting and handling of risk**[1]" and by publishing the policy, to develop the dialogue with shareholders.

Background

In his review into the quality and effectiveness of audit, Sir Donald Brydon recommended that directors present a three-year rolling Audit and Assurance Policy ("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 [the 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.

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, in relation to 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.

In order to promote engagement on company risks, Sir Donald recommended that directors should publish their statement of principal risks and uncertainties (the 'Risk Report') each year before determining the scope of the annual audit, and should actively seek shareholder and other stakeholder views on the appropriate emphasis.

To provide more insight into a company's financial resilience, Sir Donald recommended that a new 'Resilience Statement', with a demonstrable link to the 'Risk Report', should replace the existing going concern and viability statements. The Resilience Statement would address three time horizons: short, medium and long term. At present, boards are required to present the Going Concern and Viability Statements. However, even now, it is possible to present them together and include a further narrative of the risks to resilience of the business model and strategy in the long term.

In addition, Sir Donald also recommended that listed companies should publish a "Public Interest Statement" to explain how the directors view their public interest obligations and responsibilities and the actions which have been taken to meet these self-declared responsibilities. Such a statement could be used to pull together the key themes and messages from the different elements of existing ESG reporting and address considerations of the wider public interest.

See Appendix C for relevant extracts from the Brydon Review

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.

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?

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?

[1] Brydon Review – para 10.0.6

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 so that readers can understand its purpose
- 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 over 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 requirements

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.
- Describe the review process by management, and the board's oversight and challenge sufficiently to describe the reasons this is effective
- Explain the involvement of the external auditor and/or any other assurance over the process.

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

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[2].

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.

Statutory audit of the financial statements

- Describe the 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) and any specific areas of focus which the board/audit committee has requested
- Explain the fee basis for external audit work
- Describe the framework for decisions about materiality
- Indicate how shareholders should interpret the resulting audit reports

Assurance on other information in the annual report

- 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, 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 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.
  - ***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, 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.
  - ***Public Interest Statement*** – where the company has voluntarily made a Public Interest Statement, describe the board oversight process and whether it has this been subject any form of assurance.
- 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.

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.

PART 3 – the Assurance Budget

- 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
- Companies with a separate risk committee should consider including the costs of assurance around the duties of the risk committee and of the internal risk team that supports it

APPENDIX A

TYPES OF ASSURANCE AVAILABLE TODAY

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.

Limited assurance engagements are determined based on the circumstances and may include basic verification procedures such as agreeing to company information, or more extensive enquiry to independent sources and assessment of the reliability of those sources.

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

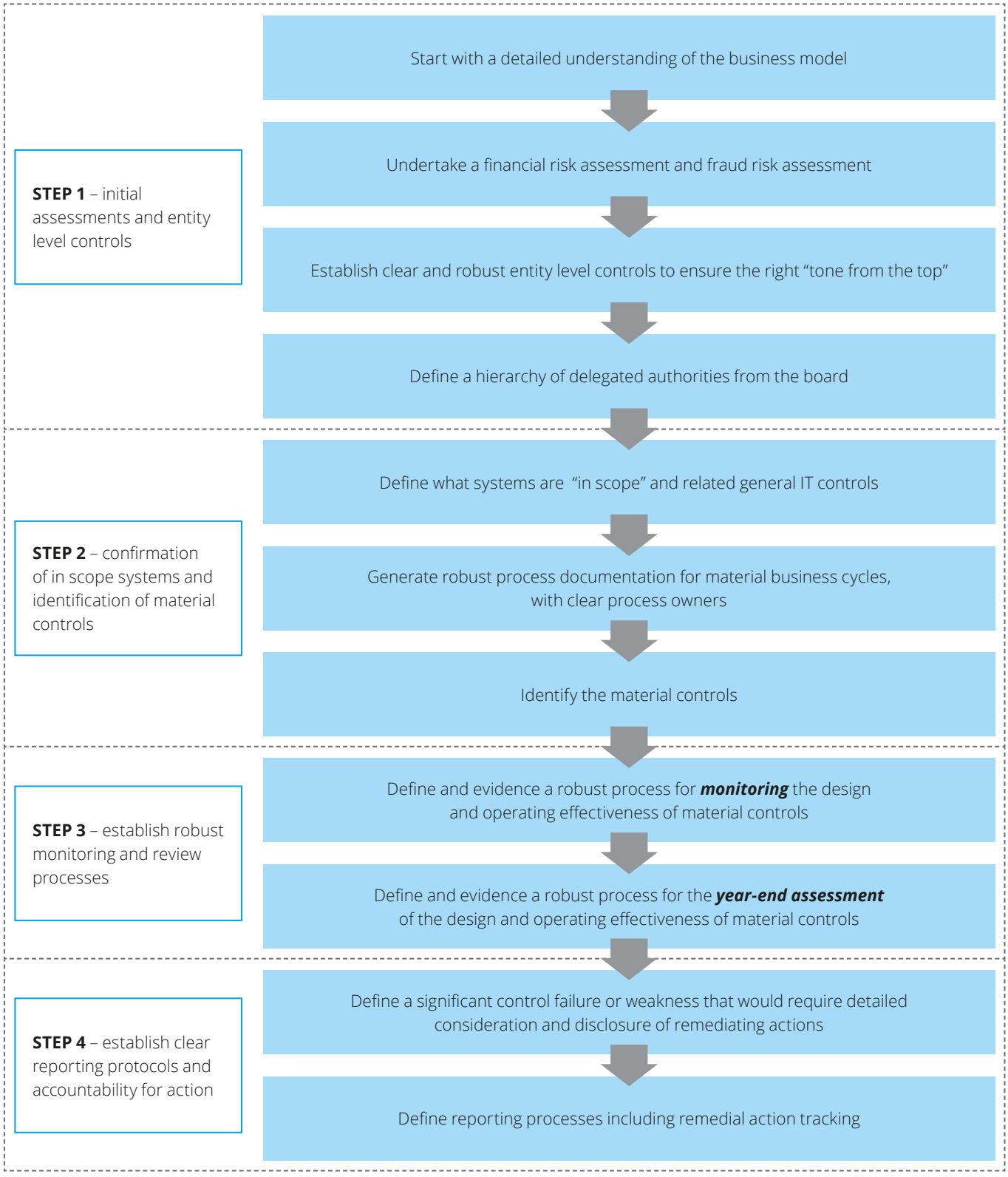
- An attestation engagement will usually involve a provider being asked to affirm an assertion made by somebody else
- A direct engagement is where the provider measures or evaluates the underlying subject matter against the applicable criteria and presents the resulting subject matter information as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

Extracts from the Brydon Review – December 2019

2.4.1 To help frame the role of the auditor(s) and to make clearer the extent of all assurance in regard to the information they [the directors] communicate, I recommend that: The directors present to the shareholders a three-year rolling Audit and Assurance Policy

2.4.2 This should indicate their approach to the appointment of auditors, the scope and materiality of all auditing (including that of the financial statements), the assurance budget and the relationship of any audit to identified risks. Shareholders would be invited to express their views on the policy in an advisory vote.

2.4.6 It will be for shareholders primarily to judge the extent to which a company's Audit and Assurance Policy enables satisfactory assurance over the Resilience Statement as a whole.

6.8.6 The auditor's opinion should state whether, based on the evidence reviewed, the directors' Public Interest Statement is presented fairly in all material respects.

10.0.3 I recommend that the audit committee publish **a three-year rolling Audit and Assurance Policy** which would be put to an annual advisory vote by shareholders for approval at the Annual General Meeting.

10.0.5 It would, inter alia,

- explain the process of appointing auditors;
- explain the work demanded of the auditors and any conditions attached;
- explain the fees basis for audit work;
- provide a framework for decisions about materiality;
- explain how seeking assurance relates to the Risk Report of the directors;
- indicate how shareholders should interpret the resulting audit reports;
- explain the approach taken to compiling the Resilience Statement and the associated extent of auditor engagement; and
- explain the approach taken to obtaining and reporting on assurance around internal controls, both in relation to the financial reporting and operational controls.

10.0.6 In doing so the Audit and Assurance Policy should encompass assurance beyond that required for the financial statements. It is here that the directors will be able to report, for example, on cyber risk and climate change impacts and explain the degree of assurance sought. The rolling nature of this Policy should also make it simple to evidence learning, and reflect changes in circumstance, from one year to the next. **This Policy provides the opportunity for companies to show how they are assuring the integrity of reporting, and handling of risk**, whether required to do so by law or not.

10.0.7 Within this policy, the assurance budget should be published, divided by broad categories of expenditure planned for the first year of the rolling three-year period covered. This budget would encompass both external fees, the cost of internal audit and any other forms of assurance that the company chooses to obtain.

10.0.8 In this way I consider it is possible to respond to those who are keen to have assurance extend to the front end of the annual report by the directors. The Audit and Assurance Policy, in describing the extent of assurance that the directors have selected, **should make clear which parts of the front end will be assured**. It will then be open to shareholders to challenge this approach. In this way proportionality is maintained in the interest of primary users; cost is not created where shareholders and directors see no value in incurring it, but where either does, then assurance can be extended. This approach also maintains the distinctiveness of the statutory audit of the financial statements as a subset of the wider audit and assurance umbrella.

13.1.13 In reporting on [the work done to monitor the company's risk management and internal control systems and review their effectiveness] boards should make clear what processes have been considered and reasons for their confidence in their effectiveness.

Deloitte.

Designed by CoRe Creative Services. RITM0579500