

# Soaring to new heights

Governance considerations for audit  
(and risk) committees with selected  
commentary from 2020 annual reports

July 2021





# Introduction

Stakeholder capitalism<sup>1</sup> and moving away from a focus on maximising shareholder value was the theme of the **Davos Manifesto 2020**. Whilst this concept dates as far back as 1932<sup>2</sup>, its more recent revival, with a specific focus on ‘people’ and ‘planet’, has reignited the debate about the role of governance and the board in the context of, what often seem like, competing stakeholder priorities. As a result, the concept of purpose as the North Star that helps navigate this complexity has come to the fore in recent years.

The changes in the UK’s governance framework resulting from the 2018 UK Corporate Governance Code (2018 Code or the Code) and Companies Miscellaneous Reporting Regulations (MRR) reflected these global trends. However, high profile business failures keep resurfacing the underlying sentiment and concerns that some critical aspects of governance are not being addressed in their entirety, or in some cases, potentially at all. These concerns were only exacerbated by the impact that COVID-19 has had on all aspects of the economy.

Contrary to the expectations of some, the much anticipated White Paper issued in March 2021 by the Department for Business, Energy & Industrial Strategy (BEIS)<sup>3</sup>, went beyond proposals to reform the audit market and product solely. Welcomingly titled “Restoring trust in audit and corporate governance”, it recognises that rebuilding public trust in business also requires changes in how the UK’s largest companies are run and the frameworks governing the oversight of directors’ duties.

Given this broadened focus on planet and people, the prospects of increasing directors’ accountability and new requirements likely to be placed on companies and those running them, we decided to shift gear this year. Instead of our traditional review of narrative reporting practice in the FTSE 350, we have instead focussed on analysing what reporting can tell us about FTSE 350 governance practices and how governance is likely to continue to evolve in light of the Government’s reform proposals, the shift towards stakeholder capitalism and the pandemic. We cover this analysis in three parts:

## Contents

<b>Introduction</b>	<b>1</b>
<b>2    Audit (and risk) committee</b>	<b>4</b>
2.1    Introduction	5
2.2    Investor expectations	8
2.3    Governance	9
2.4    Strategy – the Audit and Assurance policy	16
2.5    Risk management	20
2.6    Metrics and targets	30
2.7    Ten key questions to assess effectiveness	33
2.8    Reporting examples	34

### Part 1

To be published by September 2021. Part 1 is dedicated to the board, with a specific emphasis on governance over social, environmental and other sustainability matters.

### Part 2

This report which focuses on the audit (and risk) committee – the committee most impacted by the BEIS proposals.

### Part 3

To be published by September 2021. Part 3 will address the oversight of human capital and matters related to people, with a focus on the evolving roles of the nomination and remunerations committees.

<sup>1</sup> A form of capitalism in which companies do not only optimise short-term profits for shareholders, but seek long term value creation, by taking into account the needs of all their stakeholders, and society at large.  
<sup>2</sup> Referring to the publication, The Modern Corporation and Private Property by Adolf A. Berle and Gardiner C. Means.  
<sup>3</sup> Referred to throughout this publication as the BEIS consultation.

Each part follows a similar structure:



We start by setting the scene and cover investor expectations based on  
i) direct engagement we have had with investors  
ii) highlights on investor priorities and responsible stewardship from EY’s annual investor report.

We then provide points of view, thoughts and analysis under the broad headings of:

- Governance
- Strategy
- Risk
- Targets and metrics

supplemented with disclosure extracts from a sample of over 100 FTSE 350 annual reports (ARAs) to illustrate specific points.

We also highlight what we consider to be **‘no regret’ actions** – steps that boards can start taking now, regardless of the outcomes of the BEIS consultation.

We close with high level questions that boards and board committees can use to  
i) think about their current roles and how they may evolve; and ii) debate their effectiveness.

Our ambition is for boards and board committees to be able to use these three parts when they are debating their roles and their forward rolling agenda.

For those of you, who look forward to our annual narrative reporting analysis, we have your backs! The only new narrative reporting requirement applicable for 31 December 2021 year ends relates to companies’ disclosures against the recommendations of the Task Force on Climate-related Financial Disclosures (TCFD) and we covered this separately in our publication **“Towards TCFD compliance”** issued in May 2021. For those looking for a broader review of narrative reporting, we believe that our September 2020 report **“From intent to action”**

remains relevant. Looking back at this report, we stated that change in the governance and reporting arena and adapting to it seems to be set as a constant fixture for some years to come. This statement couldn’t be truer given the events of the last 18 months and the Government’s future agenda.

We hope that this report will therefore help boards prepare for the inevitable change that is coming.

Best regards,  
Mala and Maria



# Audit (and risk) committee



## 2.1 Introduction

The main roles and responsibilities of the audit committee (AC) are set out in Provision 25 of the Code. There are overlapping but more granular requirements (which apply on a mandatory basis rather than comply or explain) in the Financial Conduct Authority's (FCA) Disclosure Guidance and Transparency Rules (DTR) 7 and on tendering the external audit, in the Companies Act 2006. It is very telling that while the Code Provision has nine bullets, these only cover the main areas of the AC's remit.

The AC has always dealt with matters most directly linked to financial reporting and internal controls. It also oversees the risk management system in its entirety, even if other committees might have more direct responsibilities over specific risk areas.

Given the highly regulated nature of financial services, the 2009 Walker review recommended that FTSE 100 banks and insurance companies establish a separate risk committee, with responsibility for oversight of risk exposure and mitigation and for advising the board on risk appetite and tolerance.

**The majority of financial services firms (76% in our sample<sup>4</sup>) have a separate risk committee,**

---

but even aside from this sector specific nuance, the responsibilities of the AC only seem to have grown.

“

Is it time for a rethink and refresh on how the modern-day AC role and remit are captured and codified to provide an overview to boards/board committees on a) how to effectively manage the workload across committees and b) provide clarity to current and aspiring AC members on what the role involves? We talk about the audit expectation gap but are we now at risk of an expectation gap in the role of the AC?

Mala Shah-Coulon, EY, Head of Corporate Governance

There are two main reasons for this. On one hand, the complexity of matters that are in the traditional remit of the AC has increased. IT systems underpinning internal controls have become more sophisticated and the severity and occurrence of cyber attacks have gone up; international financial reporting standards increasingly involve estimation and judgements; and managing the relationship with the auditor and tendering the external audit have become more demanding as a result of regulatory requirements and scrutiny. On the other hand, new responsibilities have crept into the AC's role, sometimes because of a more or less direct link to the traditional areas e.g., dealing with non-financial reporting as an overall part of reporting and

other times purely because a topic needed “a home” and didn't fit into the agendas of any other of the board committees.

It is quite remarkable that this expansion in scope doesn't seem to have been officially “codified”. Comparing the role of the AC in the 2003 Smith Report (which is the genesis of what is in the 2018 Code and the Financial Reporting Council's (FRC's) 2016 Guidance on ACs) with the role of the AC in the 2018 Code (see **Figure 2.0**), much of what ACs are dealing with currently isn't encapsulated holistically in the DTRs, the 2018 Code or the FRC's Guidance.

<sup>4</sup> Less than 5% of the non-financial services companies in our sample had a separate risk committee. Throughout this chapter when referring to the AC, we assume that it has retained the risk oversight role.

**Figure 2.0**  
Comparing and contrasting: the role of the AC under the 2003 Smith Report versus the 2018 Code

2003 Smith Report <sup>5</sup>	2018 Code, Provision 25
The board should establish an AC, the main role and responsibilities of which should be:	The main roles and responsibilities of the AC should include:
<ul style="list-style-type: none"> <li>to monitor the integrity of the financial statements of the company;</li> </ul>	<ul style="list-style-type: none"> <li>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;</li> </ul>
<ul style="list-style-type: none"> <li>n/a</li> </ul>	<ul style="list-style-type: none"> <li>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;</li> </ul>
<ul style="list-style-type: none"> <li>to review the company's internal financial control system and, unless addressed by a separate risk committee or by the board itself, risk management systems;</li> </ul>	<ul style="list-style-type: none"> <li>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;</li> </ul>
<ul style="list-style-type: none"> <li>to monitor and review the effectiveness of the company's internal audit function;</li> </ul>	<ul style="list-style-type: none"> <li>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;</li> </ul>
<ul style="list-style-type: none"> <li>to make recommendations to the board in relation to the appointment of the external auditor and to approve the remuneration and terms of engagement of the external auditor following appointment by the shareholders in a general meeting;</li> </ul>	<ul style="list-style-type: none"> <li>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;</li> </ul>
<ul style="list-style-type: none"> <li>to monitor and review the external auditor's independence, objectivity and effectiveness;</li> </ul>	<ul style="list-style-type: none"> <li>reviewing and monitoring the external auditor's independence and objectivity;</li> <li>reviewing the effectiveness of the external audit process, taking into consideration relevant UK professional and regulatory requirements;</li> </ul>
<ul style="list-style-type: none"> <li>to develop and implement policy on the engagement of the external auditor to supply non-audit services.</li> </ul>	<ul style="list-style-type: none"> <li>developing and implementing policy on the engagement of the external auditor to supply non-audit services, ensuring there is prior approval of non-audit services, considering the impact this may have on independence, taking into account the relevant regulations and ethical guidance in this regard, and reporting to the board on any improvement or action required; and</li> </ul>
<ul style="list-style-type: none"> <li>n/a</li> </ul>	<ul style="list-style-type: none"> <li>reporting to the board on how it has discharged its responsibilities.</li> </ul>
<ul style="list-style-type: none"> <li>Where the AC's monitoring and review activities reveal cause for concern or scope for improvement, it should make recommendations to the board on action needed to address the issue or to make improvements.</li> </ul>	

<sup>5</sup> ACs Combined Code Guidance: A report and proposed guidance by an FRC-appointed group chaired by Sir Robert Smith, published January 2003.

## Main areas of the BEIS consultation impacting ACs



The proposals included within the BEIS consultation will both create new obligations on the AC and expand existing ones. With an already jam-packed agenda and meetings that can go on for many hours, ACs will need to take a long, hard look at how they prioritise to maintain effectiveness as well as consider whether and how to share some of the workload around with other committees.

\* Audit, Reporting and Governance Authority.

## 2.2 Investor expectations

Compared to the 2016 Code which stated that committee chairs should be available to answer questions at the AGM, the 2018 Code introduced a specific requirement for them to ‘seek engagement with shareholders’<sup>6</sup>, but this does not appear to have led to large scale engagement between investors and the AC Chair.

EY’s research into investor stewardship reporting and engagement has indicated that engagement on audit quality, auditor appointment and wider assurance has been low on the list of investor priorities. Based on our analysis of 2020 reporting, companies do not currently disclose much if anything on the AC Chair’s direct interactions with investors. Such engagement may exist and simply not be reported

on in the ARA, however, the lack of disclosure combined with the stewardship research indicates that it’s unlikely to be widespread. From our engagement, AC Chairs have told us that even where they had actively written to their largest investors with an offer to engage, they had not received any uptake. This was a concern raised in the Brydon review and now repeated in the BEIS consultation.

Furthermore, during informal conversations, some investors will admit that they do not read the lengthy external audit opinion and will rely simply on the fact that such an opinion, from a reputable audit firm, exists. Many add that they are put off by the length of the legalistic nature of the opinion, boilerplate wording and by the opaqueness of the conclusions disclosed in respect of key audit matters. Suggestions to rectify the situation include giving shareholders a formal opportunity to engage on risk and audit planning and ensuring greater AC Chair and auditor participation at annual general meetings (AGMs).

Investors we have spoken to recently have indicated that they would like to place more reliance on the veracity of environmental, social and governance (ESG) metrics and assumptions underpinning TCFD scenario analysis across their portfolio companies. It is therefore possible that investors will try to influence the scope of assurance ahead of the Audit and Assurance policy (A&A policy) requirement officially taking effect now that the concept has received the Government’s support.

“

Investment managers have an important role to play in the audit and corporate governance reform agenda. This will involve engaging with audit committees on material risks to the long-term value of the company. The starting point for this engagement is better disclosures on the potential risks to long-term value, through internal control disclosures, the resilience statements or the audit committee and auditor disclosures on the key audit matters or audit quality. It is critical that these reforms do not shift responsibility away from the directors — it is not the shareholders’ role to micromanage the company or direct the company to take a specific approach to audit. Directors should make the appropriate decisions for the company and be held accountable for those decisions through the normal shareholder engagement and voting mechanisms.

Andrew Ninian, Director of Stewardship & Corporate Governance at The Investment Association

“

There is a push for more engagement with investors which AC chairs support, however this requires investors to have the appropriate resources. Despite various efforts in recent years including the introduction of expanded reporting by ACs, a requirement in the Code for committee chairs to actively seek engagement, FTSE 350 ACs have not had much, if any, engagement from investors. If there is a new requirement for investors to engage and/or vote, for example when assessing the need for or value of wider audit and assurance in specific areas then to do this effectively they need to be sufficiently knowledgeable about the internal workings of companies and about the subject matter. It is not clear how this can be achieved and there is a risk that a tick box approach is adopted or voting decisions are outsourced to proxy firms. There is an understandable concern from some ACs that more information will be prepared and published with little impact on engagement levels and the ACCIF is actively working with investor groups to try to address this risk.

Alan Ferguson, Audit Committee Chairs’ Independent Forum (ACCIF), Chair of Companies & Investors Stakeholder Group

## 2.3 Governance

In the UK, current requirements governing risk management and internal control include:

- a. Under the Code – a requirement for
- ▶ The board to undertake a robust assessment of the company’s emerging and principal risks, and confirming in the ARA that it has completed this assessment, including a description of the principal risks, the procedures in place to identify emerging risks, and an explanation of how these are being managed or mitigated.
  - ▶ Establishing procedures to manage risk and oversee the internal control framework.
  - ▶ Monitoring the company’s risk management and internal control systems and, at least annually, carrying out a review of their effectiveness and reporting on that review in the annual report. The monitoring and review should cover all material controls, including financial, operational and compliance controls.

b. Under the Listing Rules (LR7.2)

For the issuer to take reasonable steps to establish and maintain adequate procedures, systems and controls to enable it [listed company] to comply with its obligations.

c. In the DTR

A description of the main features of a company’s internal control and risk management systems in relation to the financial reporting process. The company’s auditor, in turn, must state whether this is consistent with the financial statements and knowledge obtained during the audit and whether there have been any material misstatements in the information in the statement and, if so, their nature.

The extent and nature of work performed by management and boards in the UK in support of these requirements varies. It often relies on an internally defined self-assessment approach which usually does not involve detailed testing of controls nor an explicit statement over their effectiveness. Whilst undoubtedly useful, this carries with it the risk of marking one’s own homework leading to less rigour being applied. A strengthened and better codified internal control accountability framework could create discipline with regards to documentation, better ownership and responsibility for risk management and internal control processes and enhanced oversight by management and ACs.



<sup>6</sup> Provision 3 extract: ‘Committee chairs should seek engagement with shareholders on significant matters related to their areas of responsibility.’

2.3.1 Internal control systems

In light of the current UK requirements as noted above, it is not surprising that the current description of internal control systems does not focus just on controls over financial reporting, but is much broader, covering risk management and operational, as well as compliance controls. Many companies in fact refer to “internal controls *including* those relating to financial reporting process”, highlighting that these are only a subset of the overall internal control environment. Very few companies detail controls over ESG reporting.

The description of the risk management framework often explains the three lines of defence model (including the activities undertaken by each line) and the role the board and its committees play in its oversight. Companies

also describe the key features of their internal control systems, which include aspects such as established organisational structures with delegated levels of approval, manuals, authorisation procedures, codes of conduct, strategic plans and budgets. Some companies have developed internal assurance maps, which may end up being made public as part of the proposal to formulate the A&A policy (see **2.4.3** and **Intertek** example below).

Some also set out procedures that are undertaken to monitor the effectiveness on internal controls, which commonly refer to the work of internal audit, a review of actual results against budget and forecast, management meetings at various levels of the organisation and also control self-assessments, sometimes supplemented with internal audit attestation or management

certifications. Some organisations (see **Reckitt** example to the side) also have a second line of defence internal controls and compliance function that supports the first line of defence activities and often works in tandem with internal audit.

It will be important, if and when strengthened requirements over internal controls over financial reporting (ICFR) are introduced, that this broader narrative is not lost and companies continue to monitor and discuss their broader internal control systems covering operations and compliance. Not only is it required by the Code, but also it is not just failings in ICFR that can have serious consequences, as noted by **Rio Tinto** (2020 ARA, p131) weaknesses in its risk management and internal control framework contributed to the destruction of the Juukan Gorge rock shelters.

Self-assessment responses are consolidated for review at a regional level, with further review and sign-off of the consolidated self-assessments in the regional risk committees, before a final consolidated CEO and CFO review. A final summary assessment is provided to the Committee. The self-assessment exercise has been reviewed during the year to ensure global coverage and to reflect Intertek's operational and financial structure, and in order to enhance the alignment of the self-assessment to the assurance process.

**Weir** (2020 ARA, p95): The Compliance Scorecard is a control mechanism whereby each operating company undertakes self-assessments, every six months, of their compliance with Group policies and procedures, including key internal controls across a range of categories including finance, anti-bribery and corruption, tax, treasury, trade and customs, HR, cyber security, IT and legal. As far as the elements relating to finance are concerned, these cover (but are not limited to) management accounts and financial reporting, balance sheet controls, employee costs and other financial policies. Each operating company is expected to prepare and execute action plans to address any weaknesses identified as part of the self-assessment process.

Operating companies are required to retain evidence of their testing in support of their self-assessment responses. Internal audit has responsibility for confirming the self-assessment during planned visits. Any significant variances are reported to local, divisional and Group management. Any companies reporting low levels of compliance are required to prepare improvement plans to demonstrate how they will improve over a reasonable period of time. The overall compliance scores (as a percentage) are tracked over time and reported to the AC twice a year, with the Committee paying particular attention to the variances between self-assessed and internal audit assessed scores as well as trends and the performance of newly acquired companies.

**Reckitt** (2020 ARA, pp124 and 125): In conjunction with the Internal Audit team, the Corporate Control team identifies financial risks and mitigates these with appropriate internal controls, as well as establishing the minimum expected financial control requirements, applicable across the whole of Reckitt. The global financial controls framework is reviewed annually. Reckitt's internal control frameworks provide assurance that business objectives are achieved, that business is conducted in an orderly manner and in compliance with local laws, that records are accurate, reliable and free

from material misstatement, and that risks to Reckitt's assets are minimised. The Corporate Control team is accountable for managing global control policies and frameworks and for monitoring the effectiveness of the Group's internal control environment. Local markets conduct an annual controls self-assessment, comprised of over 150 system-agnostic controls across key financial processes.

Corporate Control is responsible for implementation of controls reporting and monitoring at local, Global Business Unit and global levels, working with markets to improve risk and controls capability and to support the development of remediation plans and corrective actions for control weaknesses. The Committee receives a report at each meeting summarising any controls activity since the previous meeting. Controls are monitored through, for example, regular balance sheet reviews with countries/markets and analytics, global financial controls framework submissions and monthly calls to review the status of controls. Corporate Control commenced a number of projects during the year, such as the automation of a number of manual controls by leveraging available technology and building controls capability; undertaking a readiness assessment and preparation of a proposal for compliance in anticipation of new legislation being implemented following the Kingman and Brydon reviews; and, with the Internal Audit team, the creation of a COVID-19-specific risk assessment to mitigate risks surrounding COVID-19.

**Bodycote** (2020 ARA, pp53 and 63): An annual internal control self-assessment, with management certification, is undertaken by every Bodycote plant. The assessment covers the effectiveness of key financial, compliance and selected operational controls. The results are validated by internal audit (IA) through spot checks and are reported to the Executive and ACs.

Internal auditors have received self-certification from every plant that internal controls have been complied with and noting any non-compliance. A control self-assessment has also been introduced for each of the divisional finance teams. A summary of the results was presented to the Committee. The accuracy of returns was monitored by Internal Audit by verification calls to a random sample of sites.

Examples of companies (not subject to US Sarbanes-Oxley requirements) that reference control self-assessments

**Intertek** (2020 ARA, p103): The Intertek Core Mandatory Controls (‘CMCs’) are an integral part of ‘Doing Business the Right Way’, and provide the mechanism by which we define, monitor and achieve consistently high standards in our control environment throughout the whole organisation. At the end of the year, the Committee undertook a review of the CMCs and Assurance Map to ensure that they continued to be fit for purpose. Where non-compliances with the current CMCs were identified in the 2020 internal audit review process, remediation plans have been put in place. For 2021, this process was reviewed and there were additional controls introduced to address the areas for improvement identified in 2020,

changes to existing controls in order to improve their precision, clarity and specificity with further clarity achieved by consolidating Local IT and General IT into a single integrated OneIT control set.

In order to provide assurance that the Intertek controls and policy framework is being adhered to, a self-assessment exercise is undertaken across the Group's global operations. This exercise is reviewed and refreshed each year to align to the updated control framework and to support the continued development of the Group's control environment. An online questionnaire requesting confirmation of adherence to controls: financial, operational, HR and IT is sent to all Intertek operations. Where corrective actions are needed, the country is required to provide an outline and a confirmed timeline. The results are used as an input for the Internal Audit and Compliance Audit assurance work for 2021.

### 2.3.2 Controls over financial reporting

Even though the FCA's DTR require listed (premium and standard) companies to describe the main features of their internal control and risk management systems in relation to the financial reporting process, UK companies that are not United States Foreign Private Issuers (FPIs) and do not therefore report against section 404 of the US Sarbanes-Oxley Act (US SOX), are generally less explicit than their FPI counterparts when it comes to discussing controls specifically over financial reporting. **Smith + Nephew** (see **Figure 2.1**) is an example of an FPI that provided granular detail on its ICFR. **Reckitt** (2020 ARA, pp124 and 125) is a non-FPI that included specific examples of how financial controls are monitored (annual controls self-assessments comprised of system-agnostic controls across key financial processes, regular balance sheet reviews with countries/markets and analytics, global financial controls framework submissions and monthly calls to review the status of controls).

Non-FPIs generally use internally developed frameworks to assess controls against, they seldom reference the design effectiveness of controls and statements made are often quite boilerplate. There is also no common language to categorise the severity of findings, when weaknesses have been identified and companies develop their own terms and phrases. For example, the AC of **Aggreko** (2020 ARA, p67) reviewed the remediation plan following a controls issue identified during the year in Angola, where certain month-end processes had not been completed properly for several months. These were referred to as less material control breakdowns. **Coats** (2020 ARA, p69) provided updates to the Audit and Risk Committee regarding instances where the effectiveness of internal controls were considered insufficient, including in relation to operational findings in India and the oversight of third-party contractors.

The lack of common definitions and language in the UK around internal control matters, including in respect of remediation being undertaken by management to address concerns that have been identified, is an issue. Different companies use terms, including commonly referenced 'material weakness' or 'significant deficiency' in different ways making it difficult for readers to interpret these outcomes. This will require some effort from the regulator if the BEIS proposals to strengthen reporting on ICFR come to bear.

Describing the existing internal control systems over financial reporting is not enough to ensure their adequacy. Positively, some non-FPIs recognise the need to strengthen their underlying approach to financial controls. For example, **Capita** (see **Figure 2.2**), embarked on a finance transformation programme to drive improved data quality and standardisation of activities performed by the finance community. This has included an evaluation of financial controls by the senior finance team to review the material financial controls in place for effectiveness. Non-FPI ACs should consider what measures or metrics they have in place to assess whether the outcomes of controls monitoring indicate the need for change.

### 2.3.3 Preparing for new ICFR requirements

Regardless of existing practices and requirements under the Code and DTRs, it is clear from many companies' disclosures that they feel

their existing approach to ICFR would not stand up to a 'Sarbanes-Oxley like' level of scrutiny and testing.

A number of companies have explicitly stated that they already are, or will next year, be taking action to prepare for the introduction of new ICFR requirements in the UK:

Anecdotally, some CFOs we have spoken to admit that the BEIS proposal has given them the "licence" to start implementing changes they had wanted to make for some time. They also expressed that external attestation will make things more challenging, but they see some value in it.

**Reckitt** (2020 ARA, pp124 and 125) explained that, in preparation for compliance with new legislation its Corporate Control team commenced a number of projects, such as the automation of a number of manual controls by leveraging available technology and building controls capability, and undertaking a readiness assessment for future compliance.

**ITV** (2020 ARA, p122) engaged an external consultant to perform a high level 'health check' of ITV's ICFR framework, environment maturity and readiness. The assessment considered ICFR maturity across the Group and in individual businesses, functions and other Committee of Sponsoring Organizations (COSO) categories. The assessment classified the maturity of ITV's current ICFR framework as 'developing', and concluded that processes and controls are in place in most cases, and that its control environment is broadly in line with ITV's sector and the consultant's benchmark.

Given the increased public interest in internal control systems following the Kingman and Brydon Reviews,

**Howden Joinery Group** (see **Figure 2.3**) commenced a project to review the network of internal controls in order to reappraise and document key controls consistent with responsibilities of the revised organisational structure. This project is sponsored by the chief executive officer and chief financial officer with scrutiny from the AC.

Key areas of focus for the **Synthomer** AC in 2021 will include (2020 ARA, p91) formalisation and alignment of internal control reporting across the Group to reflect the recommendations of Brydon, Kingman and the Competition and Markets Authority.

Similarly, the **Kingfisher** AC in 2021 will (2020/21 ARA, p76) "monitor plans and progress to enhance the framework for internal controls over financial reporting ahead of expected UK regulatory change towards a more SOX-like environment."

Although not explicitly referencing preparation for potential reforms, **Domino's Pizza** (2020 ARA, p91) discusses steps taken to improve its internal control environment which historically had been informal and often undocumented.

It is positive that companies are recognising the need to document, formalise and, to the extent possible, automate ICFR and are already taking action. This does however suggest that the potential gap across the FTSE 350 that

will need to be addressed if a regime similar to Sarbanes-Oxley is introduced, will likely be vast. Even more so that on the other hand, there are also a few FTSE 250 companies like **Vectura Group** (2020 ARA, p69) that do not currently have an internal audit function. Regardless of the implementation timeline, ACs should be considering now how their organisations move in incremental steps from where they are today to where they should be, regardless of the outcome of the BEIS consultation.

“

It is not enough for companies to solely focus on how controls are going to be implemented or better documented if already in place. Establishing adequate governance mechanisms to support this, including clearly defining the division of roles between the second and third line of defence as part of the assurance map, is imperative.

Neil Mathur, EY Partner, Business Consulting, [nmathur@uk.ey.com](mailto:nmathur@uk.ey.com)

Preparing to strengthen ICFR – how EY can help

Many companies that we have spoken to about the maturity of their ICFR see the BEIS consultation as a much needed catalyst for change and improvement of their control framework, regardless of its outcome.

Some are already starting controls improvement projects (as noted above) and, regardless of what the consultation outcomes may be, are focussing on establishing a robust control framework which is both efficient and assurable.

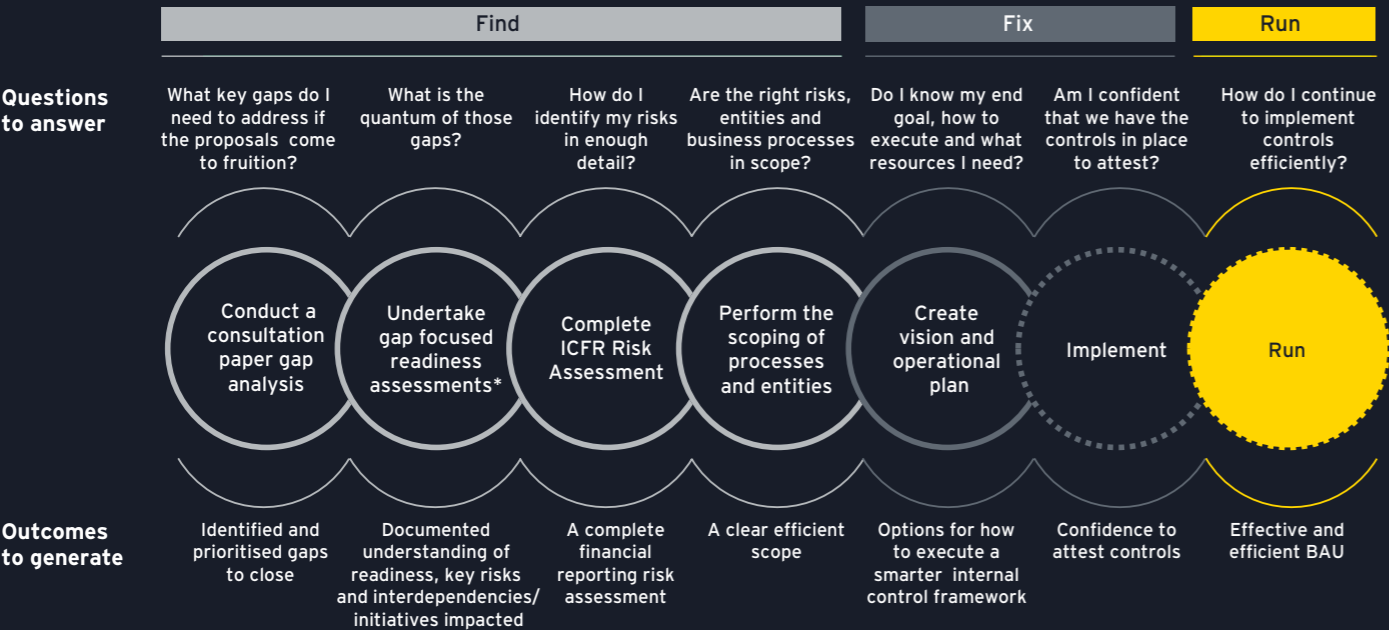
Whilst the effective date of proposed changes may seem a long way out, our experience of working with companies implementing US SOX indicates that setting up and embedding a formal, attestable controls framework can take between 18 months and three years. The main challenges companies identify include improving IT systems,

developing their assurance culture and embedding the updated control environment within the organisation.

For premium listed companies we are working with, we are following our tested, scalable approach, helping them assess their readiness, creating a vision of the desired state and starting their journey towards it. Our objective is to help companies create an efficient and effective business as usual (BAU) operating model. Our approach utilises several gap and readiness assessments to gain an understanding of gaps and readiness across key risks, IT, culture and fraud. From our discussions, there is an emerging theme of the importance of understanding IT applications, owners and the general control environments surrounding these applications. Automated controls are not only most efficient in operation, but also easier to attest.

A key element of our approach is the use of smart technology solutions from start – when scoping processes and entities – to finish when we develop risk and internal controls dashboards. These dashboards provide a real time overview of timelines, internal control testing results and remediation action plans. By analysing how risk assessments move over time, management is able to assess risk dynamically and therefore direct resources in the most efficient way.

These dashboards are responsive not just to the needs of management, but also provide ACs with a tool to help discharge their monitoring obligations and challenge management’s conclusions on ICFR.



\* IT, fraud, and risk culture

Daniel Feather, EY Partner, Assurance, dfeather@uk.ey.com

2.3.4 Controls over ESG data

Whilst we can glean some insights into the robustness of ICFR based on disclosures in annual reports, very few, if any, companies provide disclosures about the systems and processes they have in place to collate and report ESG data. From our conversations with companies, the maturity of this area varies greatly, not just between industries and geographies, but even within the same company – certain data points are accessible through established processes and trustworthy platforms whereas others are gathered manually in response to ad hoc queries.

However, the ability to reliably gather ESG data from across the organisation is no longer a nice-to-have, but is rapidly becoming an imperative. Even though it may still be some time before standards and regulatory requirements place similar onus and expectations on the accuracy of non-financial metrics as are in place for financial statement disclosures, ACs should have this topic on their agendas now. This is both in the context of beginning to develop an A&A policy and the needs of various committees that rely on ESG data for their decision making, but also in light of investors demanding data that will reliably support their investment decisions and enable their own impact reporting.

Persimmon (2020 ARA, p106) is one of the few companies that explicitly sets out its AC’s involvement in this area noting that the AC retained “a constant focus on ESG reporting through its close ties with the Sustainability Committee. In recognition of the increasing significance of ESG matters to the Group and its stakeholders, the Committee reviewed a summary report from the external auditor on the current ESG reporting framework. This report has enabled the Committee to assess the Group’s existing disclosures and evolutions in sustainability reporting, and support ongoing preparations for future reporting obligations (...).”

This is also an area of increasing regulatory interest. The FCA’s **Primary Market Technical Note** of December 2020 emphasises that listed companies need to have the right systems in place for the collection of material ESG data:

*“In considering whether their procedures, systems and controls are adequate to enable them to comply with their obligations under these various regimes, including the timely and accurate disclosure of information to the market, an issuer should consider whether there is a need to access and draw on specific data sources when disclosing climate-related and other ESG-related risks and opportunities. An issuer should also consider whether there is a need to develop specific systems, analytical instruments or organisational arrangements to collate and assess the information required to enable it to comply with its obligations.”*

This is consistent with advice from the Sustainability Accounting Standards Board (SASB) that ACs should review the effectiveness of the company’s internal controls over sustainability information gathering and reporting to ensure it is comfortable with the quality and reliability of the data<sup>7</sup>.

There is however a risk that, as companies start to focus on ICFR, improving the maturity of processes and controls underpinning ESG data will take a temporary backstep. The Institute of Internal Auditors’ White Paper “**Internal Audit’s role in ESG reporting**,” published in May 2021 provides useful suggestions on internal audit’s role in establishing a functional ESG control environment. ACs may want to consider how to build in some of the observations into the internal audit annual plan.

Reporting against the requirements of the TCFD

Linked to controls over ESG data is the consideration of the role the AC needs to play with regards to TCFD reporting. The Canada Climate Law Initiative issued a guide for boards of directors focussing on ACs and Effective Climate Governance<sup>8</sup> in which it explains that the AC’s role, at various points in an organisation’s maturity, may include:

- ▶ Setting the stage for integrating accountabilities around climate change and the overall maturation of climate risk management.
- ▶ Initiating the identification of financial risks that arise as a result of physical and transition risks, which will facilitate comprehensive valuation of financial risk.
- ▶ Incorporating a climate change lens across the three lines of defence: business ownership, risk management and oversight of internal audits.
- ▶ Validating and incorporating climate-related financial disclosures within the suite of corporate disclosure, noting that accurate and complete climate-related data is key to ensuring that disclosure standards are met.

With the above in mind, the AC will need to consider how oversight of the new requirement for TCFD reporting will fit into its existing remit and require coordination with other board committees if relevant. It will also need to give this reporting due consideration when developing the A&A policy (see **section 2.4**).

ACs may find our publication “**Towards TCFD compliance**” which contains observations, insights into developing practice, and noteworthy examples from 31 December 2020 reporters useful.

<sup>7</sup> SASB, ‘Connecting Business and Investors on the Financial Impacts of Sustainability’, (February 2020),  
<sup>8</sup> CCLI-Guide-for-Audit-Committees-on-Climate-Governance-December-1-2020.pdf (ox.ac.uk).

## 2.4 Strategy – the Audit and Assurance (A&A) policy

Most ACs will already have a well understood, even if not documented, approach to assurance. The A&A policy, if introduced, will however have a dual purpose.

On the one hand, it will need to be an effective tool for the board to assess the adequacy of the existing

assurance arrangements over matters of strategic importance, given evolving stakeholder expectations. On the other, it will need to be formulated in a manner that will facilitate engagement with investors on what can be perceived as a somewhat dry and technical topic.

### 2.4.1 Proposed content of an A&A policy

The BEIS consultation proposes that the A&A policy covers the following three pillars:

1

What, if any, independent assurance the company intends to obtain beyond that required for the financial statements, at a minimum providing an explanation of the independent assurance approach in respect of the resilience statement and the effectiveness of the company's internal controls framework (external assurance pillar);

2

A description of the company's internal auditing and assurance processes (internal assurance pillar);

3

A description of external audit tendering policies (external audit pillar); and this should be underpinned by an explanation of how shareholder and employee views were considered in developing the A&A policy.

### 2.4.2 Defining assurance in the context of the A&A policy

As noted by the Institute of Chartered Accountants in England and Wales (ICAEW) in its publication<sup>9</sup>, the word assurance as a professional concept does not have a universally agreed definition. The understanding of terms such as 'limited' or 'negative' assurance varies greatly outside of the auditing profession, as does knowledge of what assurance standards<sup>10</sup>, such as the International Standard on Assurance Engagements 3000 (Revised), actually entail. The landscape gets further complicated, when internal assurance activities from the second and third line of defence are thrown into the mix. In addition, consideration needs to be given to reporting areas, such as the viability statement or s172 statements, that neither have a track record of having previously been assured nor any clear standards/ methodology against which assurance procedures could currently be conducted, and new reporting requirements, like TCFD, where a broader approach to assurance beyond greenhouse gas emissions is still nascent.

ACs will therefore need to oversee the development of a commonly understood vocabulary that will allow the organisation to define the level of assurance that it obtains from various internal and external sources and how that matches up both against risk of fraud and error as well as the importance various stakeholders attach to the area of external reporting.

### 2.4.3 What steps can be taken now

Whilst the ultimate content of the A&A policy is yet to be determined, as is the form and frequency of investor engagement thereon, there are a number of steps we recommend that ACs and boards can take now in order to prepare. We consider these to be in the spirit of good governance, regardless of whether the requirement for an A&A policy ultimately comes to fruition:

1

#### Re-assess your risk framework

The robustness and the effectiveness of the risk management framework is in itself an entity level control in the management of an organisation's risk. The level of disruption from the COVID-19 pandemic called into question traditional risk management models and highlighted the need to supplement the annual process with more real-time information. Some companies, like **Vodafone** (2021 ARA, p58), are already undertaking activities to strengthen their risk framework. Vodafone references, amongst others, improving the process for the identification and assessment of emerging risks; enhancing the process of collecting key risk indicators and monitoring early-warning signals in both the internal and external environment; as well as defining a more dynamic approach to risk identification, assessment and escalation.

A pivot towards a more agile approach not only helps manage downside, but by accelerating responsiveness allows organisations to take advantage of opportunities as well. ACs may therefore want to commission a review of the existing framework which could include benchmarking against the principle based risk management standards ISO 31000 (and in the future ISO 31050<sup>11</sup>). Such benchmarking would additionally provide comfort in respect of the long-term part of the resilience statement.

<sup>11</sup> ISO 31050 – 'Guidance for managing emerging risks to enhance resilience' is aimed to be published in mid 2021.

2

#### Ask the auditor to explain in detail procedures performed over the viability statement

While auditing standards specify the work auditors must perform over the going concern assertion, this isn't so for the viability statement. However, as the Listing Rules specifically require the auditor to review the viability statement and conclude whether it is materially consistent with the financial statements and knowledge obtained during the audit, audit firms have developed their own work programmes addressing this area. If not already being done, the AC should request that the auditor provides a detailed explanation of the procedures it undertakes. This will allow the AC to think through its approach over external assurance over the viability statement.

3

#### Understand the scope of internal control considerations

In order to implement appropriate internal controls, management breaks down the principal risks into detailed risk factors mapped against the processes they are associated with. For example, a principal risk related to human capital may be underpinned amongst others by payroll and pensions (financial processes), recruitment and retention (operational processes), data protection (compliance processes) and payroll software (IT system). ACs may want to discuss a summary of this mapping and the materiality of related flows with management to refresh their understanding of the scope of internal control considerations. The maturity of controls over non-financial areas will impact the assurance readiness of related disclosures. We discuss the key considerations regarding ICFR in **section 2.3.3** above.



<sup>9</sup> Developing a meaningful Audit and Assurance Policy | ICAEW.  
<sup>10</sup> Standards and guidance | ICAEW.

# 4

## Determine disclosures of strategic importance to stakeholders that are not covered either by the statutory auditor or other external assurance providers

One of the underlying reasons for Brydon recommending the introduction of an A&A Policy was to close the expectations gap as it related to the level of assurance over disclosures within the front half of the annual report as well as other aspects of corporate reporting. We would therefore recommend a workshop, attended at a minimum by representatives of all the board committees and the executive, with an objective to identify:

- Disclosures in the front half that are not already in the scope of the audit, but are likely to be of higher importance to stakeholders (e.g., non-financial KPIs, greenhouse gas emissions). **Unilever** has material metrics from its Unilever Sustainable Living Plan independently assured (2020 ARA, p71 and see **Figure 2.4**), and **AstraZeneca** (2020 ARA, p275) lists out sustainability information contained within its ARA over which limited external assurance has been provided.
- Reporting outside of the ARA, such as Modern Slavery or sustainability reports/TCFD reports (where separately produced), to which assurance could add veracity and reliability.

Where available, use existing stakeholder materiality maps. Such a workshop could also be an opportunity for a spring clean – we encourage companies to revisit the content of the front half and assess whether any disclosures could be streamlined or removed before deciding whether to incorporate other disclosures that are of higher strategic relevance to stakeholders.

# 5

## Understand the assurance readiness of the disclosures and prioritise

Based on the steps above organisations should create or update existing assurance maps – setting out the existing assurance over key risks and identified disclosures, including clear roles and responsibilities. Where identified disclosures are not already being assured externally, this will allow for their assurance readiness to be assessed. Mapping the disclosures on a two by two model with assurance readiness on one axis and stakeholder materiality on the other can help prioritise which areas to focus on first.

# 6

## Commence initial investor engagement activities on draft A&A policy

As noted earlier, there is limited evidence of investors engaging with companies on matters of assurance and therefore expect that ACs may not have a formed view on what their shareholders expect. We therefore recommend that the Head of Investor relations supports the AC Chair in organising a formal engagement event on the topic. This initial feedback will help the AC shape its approach to broader assurance and its thinking on formulating the A&A policy and refine scoping and priorities. It may also provide insights about additional disclosures, e.g., in respect of internal controls or fraud assessment, that investors would value being incorporated into the ARA now. The outcomes of this engagement can be reported on as part of the section 172 statement and/or application of Principle D of the Code.

It is difficult to predict to what extent shareholders will become involved in influencing the A&A policy beyond the more obvious areas such as ESG metrics included in executive remuneration or progress against decarbonisation targets. However, the recent ‘say on climate’ movement indicates that investors are expanding how they use their voting powers.

In our view it is therefore important for companies to keep track of the topics on which investors have directly engaged, as this could identify their key areas of interest and/or concern and in turn influence assurance priorities/requests. It is possible that investors will push for additional assurance in areas where they believe a company’s reporting is not sufficiently transparent.

# 7

## Assess the need for assurance over internal reporting

Whilst the focus of the A&A policy is firmly on external reporting, we would encourage directors to consider the existing governance over information presented to the board and its committees for the purpose of decision making. We expect that there is likely to be a degree of overlap, for example in respect of metrics relating to executive performance and remuneration, but there might also be information such as key risk indicators or metrics within culture dashboards that are not publicly disclosed but are relied on by directors in discharging their duties.

# 8

## Analyse existing capabilities and capacity and determine who your strategic assurance providers are

It is unlikely that companies will conclude that they should reduce the scope and extent of assurance they currently obtain – quite the contrary. It will therefore be important to determine what additional resource will be required to meet the new assurance needs whether internal, external, or most likely, a combination of the two.

Where third-party support will be required, the AC will need to consider potential providers in the context of non-audit service restrictions and maintaining independence given the timing of upcoming external audit tender activity. This will become additionally complicated by the proposed introduction of shared audits.

“A number of FTSE 350 companies are already planning their A&A policies and have asked me for views on how they should go about this. Firstly, it is important not to lose sight of its objective – this is firmly linked to disclosures and explaining to stakeholders the AC’s policy on assurance over those, such that stakeholders can form a view for themselves on the veracity of those disclosures that are material to them.

Given this, and on the basis of the current BEIS proposals my recommendation would be for the core of the A&A policy to explain the combination of external and internal assurance over material disclosures by topic area rather than by the type of assurance that is being obtained:

### ICFR

If companies are not obtaining independent assurance over ICFR, provide an explanation of how directors plan to assure themselves that it is appropriate to make a statement on the effectiveness of ICFR. Ideally, I would therefore expect detail on the specific second and third line of defence activities and the AC’s oversight of these

### Resilience statement

I would caution companies against discussing assurance over the resilience statement overall but instead identifying its various constituents and addressing those in turn. For example, you may get an external third party to benchmark your risk framework against risk management standards; your internal audit team to assure the controls over the forecasting process that underpins the viability model; and the external auditor to check consistency between the base case used in going concern and viability modelling.

## Metrics: Non-financial information and Additional Performance Measures (APMs)

For all metrics that the A&A policy will address, make sure that there is clarity over scope and where they are disclosed (front half of ARA, sustainability report, other) and that any “groupings” do not create ambiguity.

For metrics that are independently assured, set out the assurance provider and the level of assurance that they provide. For material metrics assured internally, explain the basis for this choice, and whether this approach is expected to evolve over the next three years. APMs that are included in the front half, will be covered by the consistency check the external auditor performs against the financial statements, but for APMs outside of this, set out your assurance approach.

### Other considerations

For information extracted from one source and summarised and replicated across a number of documents consider explaining how consistency with the source of the disclosure has been ensured. If you are not obtaining a review opinion from your external auditor on your interim financial information, you may want to consider explaining the reason for this.

The process information on internal assurance and the external audit can then be provided separately. A lot of the content might already be included in the ARA. When deciding how much detail to include on internal assurance, keep in mind the core objective of the policy as I note above and how this part of the narrative will aid the reader’s understanding of it.”

Maria Kępa, Director, EY Corporate Governance Team

## 2.5 Risk management

The Cadbury Report published in 1992 which forms the genesis of various iterations of today's UK Corporate Governance Code only briefly mentioned risk management as one of the matters to be included on the board's schedule. This did not change much until the 2010 version of the Code which introduced enhanced reporting in relation to risk management.

Since then, the focus on risk has steadily increased, with the 2014 Code introducing the viability statement and the 2018 Code introducing obligations regarding emerging risks. It is therefore not surprising that oversight of risks takes up a substantial portion of an AC's time (see example in **Figure 2.5**).

76% of financial services companies within our sample and 4.5% of companies from other industries had established a separate risk committee.

Of those that did not, around 18% refer to the committee as the Audit and Risk committee.

### 2.5.1 Resilience

The requirement for a "longer term viability statement" was first introduced in the 2014 Code, following the recommendations of the Sharman Inquiry which was set up as a result of the financial crisis of 2008 and the unexpected failure of businesses previously thought to be sound and resilient.

The very brief provision was supplemented by the FRC's Guidance on Risk Management, Internal Control and Related Financial and

Business Reporting. Unfortunately, the practical application of this requirement has been found wanting, with many investors feeling that it has not resulted in any real change in their understanding of how a company's board thinks about longer term prospects nor their preparation for longer term challenges, but rather as yet another compliance hurdle to overcome.

Reflecting this sentiment, the Kingman review published in 2018 concluded that viability statements needed to be reviewed and reformed, or abolished. The risk of businesses failing as a result of the COVID-19 pandemic brought the viability discussion to the fore again in 2020.

*"There is strong investor and wider stakeholder interest in how companies are building business resilience to cope with severe yet plausible scenarios in the short and medium term, and in understanding how a company's directors are exploring and*

As set out in our publication "**Preparing your interim narrative under COVID-19**", the going concern notes in the 31 March 2020 reports we reviewed took on many of the characteristics of a viability statement, with references to 'severe but plausible downside scenarios', 'reverse stress testing' along with setting out mitigating actions available to management. The narrative was extensive, even in the case of companies where there was no material uncertainty regarding going concern — so as to assure investors that the issue has been examined closely. Even though, just three months later, June 2020 reporters were already preparing a more slimmed down version with fewer companies including a quantification of the estimated impacts of COVID-19 scenarios, these were still significantly more informative than disclosures in previous years.

*preparing for likely challenges over the long term. Better disclosures of management thinking on resilience enable better informed investment decisions which can lower the cost of capital."* Para 3.1.6, BEIS consultation

With the backdrop of COVID-19, it can hardly be surprising that the Government has decided to take forward the recommendation from the Brydon Review of introducing a resilience statement, rather than outright abolishing the viability statement. The proposal, as it relates to the medium term viability, is more prescriptive than current requirements, introducing a minimum five year period, the inclusion of at least two reverse stress testing scenarios and a list of matters (subject to consultation), including climate change risk, that should be specifically addressed in the statement. The consultation does not go as far as to mandate specific auditor reporting on the statement,

but suggests that this should be an explicit part of the A&A policy.

One conclusion that might be drawn from the failure of the viability statement to meet investor expectations and the swift contraction of reporting on viability and liquidity under COVID-19 is, that despite investor and wider stakeholder interest in the topic, companies prefer not to be overly transparent about their modelling and its outcomes if they can help it, potentially being worried about a negative market reaction that 'oversharing' might bring in a BAU environment.

Another conclusion might be that companies are continuing to struggle with the concept of aggregating risks into plausible scenarios and determining what level of aggregation remains relevant and at what point it becomes a remote 'doomsday' scenario. The ICAEW article on reverse stress testing, whilst useful, is still highly theoretical.<sup>12</sup> Unless there is clear guidance on how to perform reverse stress testing for companies outside the financial sector, the BEIS proposal to introduce two mandatory reverse stress tests might add to the confusion. The FRC's project to explore both climate and non-climate applications of scenario analysis by FTSE 350 companies that is being led by the Alliance Manchester Business School<sup>13</sup>, may potentially bring some clarity.

It is therefore uncertain whether the BEIS reform proposals will help address the root causes for current reporting not meeting stakeholder expectations. Mandating which matters should be included by all companies seems to go against the notion of linking viability to principal risks and high impact, low probability events specific to the entity, and may, in fact, make creating plausible scenarios more complicated and increase boilerplate disclosure.

Instead of introducing a new resilience statement, we would advocate that the requirements underpinning the current Provision 31 (which interestingly do not even mention the term viability) are made more granular and include the minimum steps that companies must take to fulfil that Provision and some mandatory disclosures that must be made by all companies e.g., the scenarios that have been modelled and how these map to principal risks, as is done by ITV within the viability statement (see **Figure 2.5**) or by BAT within the principal risk section of its annual report (BAT 2020 ARA, pp84-88). Furthermore, we would recommend that ACs on an annual basis review, challenge and approve supporting internal documentation that adequately explains the approach underpinning the viability modelling, including why, if relevant, certain principal risks were not factored in (see example structure below) and that the regulator review such documentation on a sample basis in a similar vein to the review of audits on a cyclical basis.

#### 2018 Code Provision 31

Taking account of the company's current position and principal risks, the board should explain in the annual report how it has assessed the prospects of the company, over what period it has done so and why it considers that period to be appropriate. The board should state whether

it has a reasonable expectation that the company will be able to continue in operation and meet its liabilities as they fall due over the period of their assessment, drawing attention to any qualifications or assumptions as necessary.

<sup>12</sup> **Coronavirus (COVID-19): Introducing reverse stress testing | ICAEW.**

<sup>13</sup> **Financial Reporting Council commissions AMBS for major study | Alliance MBS (manchester.ac.uk).**

**Vodafone** (2021 ARA, pp64-67) included the impacts of each principal risk in the form of a scenario explanation within their risk report. Some companies – like **Reckitt** (see **Figure 2.6**) – have started reporting on interconnectivity of their principal (and emerging) risks. Such an analysis should help to determine how to aggregate risks, or their constituents, into scenarios. **Meggitt** (see **Figure 2.7**) disclosed risk velocity, an important dimension for consideration when modelling the risk impacts.

Despite the FRC’s Guidance and clarification from the FRC Lab<sup>14</sup>, the two-step approach of first discussing longer-term prospects (followed by viability) has not gained traction. There are few companies like **St. James’s Place** (see **Figure 2.8**) that discuss resilience over the viability period and then more broadly over an unspecified period in the longer term. It is unclear exactly how the proposed long-term section of the resilience statement would differ from existing mandatory business model disclosures and the market context narrative that many reporters

already include. For example, **RSA Group** (2020 ARA, pp12 and 13) provides insightful forward-looking market trend explanations. If the requirements are introduced as drafted, we foresee a risk that existing disclosures are simply amalgamated into one section and shifted around the ARA, rather than making a difference in substance. Most importantly, what ACs cannot lose sight of, is that the process underpinning the disclosures related to viability (as currently) or resilience (in the future) cannot be limited to

identifying those situations that might undermine a company’s viability, but should assist directors in assessing whether the approach to preventing those situations or mitigating them when they arise, is adequate. We recommend that ACs use this year to consider the robustness of the process underpinning the preparation of the viability statement and the documentation that supports it, including in the context of developing the A&A policy. This should also be an opportunity to re-challenge the

scenarios and, where the current viability period is less than five years, explore the level of confidence that management would have in extending the period should the Government’s proposals materialise. Directors should also extrapolate the learnings from the pandemic to assess how good the company is at crisis management. The AC should ensure that minutes from its meeting(s) clearly capture the challenges it made and the questions it asked of management in respect of its paper supporting the viability assessment.

Example: Structure of management’s paper to the AC supporting the viability assessment

1	Background	5.3	Discussion of liquidity and covenant headroom
2	Viability period assessment	6	Quantifying Plausible Downside Scenarios (PDS) for each scenario modelled:
3	Identifying risks with the potential magnitude to individually, or in combination with other risks, threaten viability:	6.1	Explanation of the scenario, including consideration of strategic, commercial and financial risks/challenges
3.1	Updating the risk assessment	6.2	Discussion of risk appetite, proximity, velocity
3.2	Justification for principal risks excluded from the assessment	6.3	Approach to ‘doomsday’ scenario (risk aggregation)
3.3	Review of remaining interconnected risks, including emerging risks, that could augment the impact of a principal risk-based scenario materialising	7	Modelling and headroom considerations
3.4	Assessment of potential singular/idiosyncratic events not covered by 3.2 and 3.3 (e.g., due to lower probability)	7.1	Impact of key sensitivities on base case forecasts
3.5	Matters impacting risks specific to the current year (e.g., COVID-19 pandemic considerations)	7.2	Impact on liquidity and covenants
4	Breaches leading to viability threats (e.g., liquidity, covenants, other defaults)	7.3	Impact on covenants
5	Base case forecast:	7.4	Identification and quantification of mitigating actions to offset downside sensitivities
5.1	Overview of forecasting process	7.5	Early indicators of the need to undertake mitigating actions and their monitoring
5.2	Key assumptions in the base case forecast (e.g., trading, working capital, capital expenditure and financing)	8	Reverse stress test (RST)
5.3	Major liquidity events (e.g., debt repayment falling due with the viability period)	8.1	Assumptions underpinning RST
		8.2	Comparison between PDS headrooms and RST
		8.3	Overall view on the resilience to the threats to viability
		9	Crisis management
		10	Proposed viability disclosures in the ARA including how the disclosures have evolved since prior year

Reminder: Hallmarks of a meaningful viability statement

By reference to guidance from the Investment Association <sup>15</sup> , the FRC Lab <sup>16</sup> , the FRC’s more recent COVID-19 related publications <sup>17</sup> and our own views as expressed in previous publications, below are the hallmarks of a meaningful viability statement:	<ul style="list-style-type: none"><li>▶ Be clear on any other overarching qualifications, including your approach to aggregating scenarios/“doomsday” considerations.</li><li>▶ Explain your scenarios (see <b>Hammerson</b> and <b>ITV 2020 ARAs</b>)<ul style="list-style-type: none"><li>▶ Clarify which principal risks influenced the scenarios and whether any low probability, high impact events have been considered;</li><li>▶ Ensure scenarios provide sufficient detail to “tell a story”;</li><li>▶ Describe the outcomes of scenarios, including the plausibility of any reverse stress testing scenarios materialising.</li></ul></li><li>▶ Set out mitigating actions available to management (see <b>Fresnillo 2019 ARA</b> and <b>Severn Trent 2021 ARA</b>)</li></ul>
<ul style="list-style-type: none"><li>▶ Discuss prospects separately from viability; explain using cross referencing where relevant (see <b>Equiniti</b> and <b>St. James’s Place 2020 ARAs</b>):<ul style="list-style-type: none"><li>▶ How resilient and adaptable to risks your business model is;</li><li>▶ Which of your principal risks could undermine your current business model rather than just impact performance; and</li><li>▶ How you might be impacted by emerging risks.</li></ul></li><li>▶ Explain the period chosen for the viability assessment (see <b>Next 2021 ARA</b>)<ul style="list-style-type: none"><li>▶ Ground the explanation in industry considerations; and</li><li>▶ Include company specific factors and co-relate to other periods referenced within the ARA e.g., expiry of lease term, average duration of long term contracts, forward land supply.</li></ul></li><li>▶ Set out the approach to the assessment (see <b>Equiniti</b> and <b>Rolls Royce 2020 ARAs</b>)<ul style="list-style-type: none"><li>▶ Explain the interaction between going concern and viability modelling;</li><li>▶ Set out the key assumptions underpinning the base forecast; and</li></ul></li></ul>	<p>As noted earlier, the BEIS consultation suggests that the resilience statement should be one of the areas explicitly covered by the A&amp;A policy. Although directed at its members, the Investment Association’s paper written in collaboration with EY, <b>Effective Governance of Operational Resilience</b> could provide useful inspiration for companies in respect of practical steps they can take to assess the effectiveness of their governance framework in respect of operational resilience.</p>

<sup>14</sup> Lab project report: Risk and viability reporting (November 2017).

<sup>15</sup> The Investment Association Guidelines on Viability Statements, November 2016.

<sup>16</sup> Lab project report: Risk and viability reporting, November 2017.

<sup>17</sup> COVID-19 – Going concern, risk and viability. Reporting in times of uncertainty, Financial Reporting Lab, June 2020.

2.5.2 Renewed emphasis on tackling fraud

The impact of fraud on the economy is significant. According to the Association of Certified Fraud Examiners (ACFE) 2020 Report to the Nations, Certified Fraud Examiners<sup>18</sup> estimate that organisations lose 5% of their revenue to fraud each year. Projected against 2019 Gross World Product (US\$90.52 trillion), that's more than US\$4.5 trillion lost to fraud globally each year. These impacts are only likely to increase due to the economic uncertainty brought on by the COVID-19 pandemic and the proliferation of remote working environments limiting management's oversight, bringing the fraud triangle of pressure, incentive and opportunity to the fore once more.

The BEIS consultation proposes that directors report on the steps they

have taken to prevent and detect material fraud and the auditor to report on the work performed as part of the statutory audit to conclude whether the directors' statement is factually accurate. In addition, the obligation on the auditor to detect material fraud is going to be strengthened.

Given these proposals and more generally, the increasing scrutiny being placed by investors and other stakeholders in this respect, we expect that many directors will need to take a step back and challenge the basics of their companies' fraud management framework. This is if one in fact even exists, as fraud remains a multi-faceted conundrum that many entities struggle with for a number of reasons.

Firstly, there are many different ways in which organisations can

categorise fraud; one of the ways is to think of fraud:

- In the business – relating to areas such as financial reporting;
- On the business – for example the misappropriation of assets, whether by internal or external agents; or
- By the business – covering aspects such as bribery and corruption.

Companies, especially those outside of financial services, seldom explicitly reference fraud risks and fraud assessments in their ARAs, and when they do, disclosures predominantly relate to compliance risk and fraud by the business. This is despite the fact that based on speaking to businesses, actual focus is very often on fraud on the business. Fraud in the business is rarely mentioned, despite so many high-profile company failures having

involved fraudulent accounting. Few companies, unlike **Grafton** (see **Figure 2.9**), specifically reference conducting fraud risk assessments to help identify additional anti-fraud controls. **IAG** (2020 ARA, p120) goes a step further, with the AC referencing results of focused anti-fraud control internal audits in its report and requesting management to identify additional sources of fraud detection assurance going forward.

Secondly, due to these multiple layers, fraud risk is typically addressed by a hybrid of different functions such as procurement, human resources and compliance. This makes oversight from those charged with governance more challenging than in some of the other areas of increasing emphasis such as cyber security. It is therefore likely that over the next few years as directors seek ways to meet

the new proposed requirements, more entities will adapt to a single owner of fraud risk. That being said, ensuring responsiveness to fraud risk assessment will continue to require bringing together various roles and functions from the business and assessing the fraud risks on a continuous basis as part of the overall ERM approach.

Thirdly, directors need to define their fraud risk appetite and translate that into their definition of what is material fraud in the context of the business. This is a complex and subjective issue; a small facilitation payment made to secure a contract may have material consequences in relation to regulatory scrutiny, fines, reputational damage and potentially even result in the loss of licence to operate. In other cases, such as described by **RHI Magnesita** (see **Figure 2.10**), fraud can go

unchecked and impacts accumulate for many years. These materiality considerations will influence how the sensitivity of both prevent and detect controls over fraud risks is calibrated which may need to be different to that set for other elements of ICFR.

It is worth adding that explaining how the board has discharged of its duty to monitor culture will need to be inherently linked to any future reporting by directors on the steps they have taken to prevent and detect material fraud. After all, having an embedded culture that empowers employees to speak-up is a powerful tool for fraud detection; having an embedded culture that creates a strong, common belief in what 'doing the right thing' means, will help prevent it from happening in the first place.



Examples of controls supporting fraud prevention and detection

Control	Prevent	Detect
<b>Risk assessment:</b> In order to implement adequate controls, directors first have to identify and articulate their fraud risks and fraud risk appetite. Unless real-time data is considered in fraud risk assessments, they quickly become outdated and siloed from day-to-day business operations.	✗	
<b>Policy setting and standard setting:</b> Fraud policies are often cumbersome, complicated and checklist orientated. Policies are most effective when they are clear, understandable and principle orientated rather than prescriptive in format. Training and awareness should be provided to employees, with enhanced training for employees in higher risk roles.	✗	✗
<b>Whistleblower hotline:</b> More than 40% of cases in the 2020 ACFE study were uncovered by tips, so the importance of this control cannot be underestimated. <sup>19</sup> Entities should raise awareness of their whistleblower hotline, and issue formal statements to limit the fear of retaliation concerns amongst employees.	✗	✗
<b>Management and control processes:</b> An entity should have clear guidance over roles, responsibilities and accountabilities. Controls need to be designed with specific fraud considerations. Automated controls are more effective at preventing fraud.	✗	
<b>Data analytics:</b> Digital disruption has created an expectation that businesses will use data to identify and monitor fraud risks, as noted in the US Department of Justice's guidance "Evaluation of Corporate Compliance Programs" issued in June 2020. Monitoring through the use of data should take place pro-actively with predictive trends analytics and/or artificial intelligence, and not only through retrospective testing.		✗
<b>Fraud response plan:</b> When a fraud incident occurs, it is important to conduct an investigation, followed by a root cause analysis and remediation process. Lessons learnt should be shared amongst the business to raise awareness and act as a deterrent.		✗

<sup>18</sup> 2020 ACFE Report to the Nations.

<sup>19</sup> For features of a well-designed whistleblower helpline see <https://www.thecaq.org/wp-content/uploads/2019/03/the-fraud-resistant-organization.pdf>.

## Preventing and detecting fraud – how EY can help

Our experience of where we have seen fraud risk assessments carried out well is when the business properly engages with the issues, where 'grey areas' are identified and debated, where the different nature of fraud risk is identified and taken into account in the assessment, and where it is being sponsored at an appropriately senior level.

To assess the maturity of a company's fraud risk framework, we use EY's Fraud Risk Management Framework (FRAME) – a guided questionnaire featuring 36 questions based on the most recent ACFE/COSO fraud guidance with a bespoke weighting system. Common findings from deploying FRAME may include:

- ▶ The need for a more detailed fraud risk assessment and controls mapping at a business unit/geography/activity level;
- ▶ Developing a fraud policy, incident management plan and/or fraud response plan;
- ▶ Developing initiatives to raise awareness of fraud across business units;
- ▶ Enhancing third-party risk management processes; and
- ▶ Assessing and strengthening fraud control and monitoring programmes.

EY's Fraud Risk Management Framework



Jonathan Middup, EY Partner,  
Forensic & Integrity Services,  
jmiddup@uk.ey.com

### 2.5.3 Oversight over cyber resilience

#### Cyber security as a principal risk

According to **RBC Global Assets Management's 2020 Responsible Investment Survey**<sup>20</sup>, cyber security is among the top five investor concerns. This is hardly surprising given four in 10 UK businesses (39%) have reported some kind of cyber security breach or attack in the last 12 months.<sup>21</sup>

This is nothing new – cyber security has represented a critical challenge for most organisations for a number of years. Around 80% of the companies within our sample had a cyber security related principal risk, with a further 12% explicitly referencing cyber security as part of operational risk (financial service companies) or business interruption/continuity (**Derwent London**, see **Figure 2.11**).

To ensure that due attention is given to this matter, some boards go as far as linking executive remuneration to the achievement of cyber security improvements. For example, the **London Stock Exchange Group** (2020 ARA, p106) includes two performance measures related to cyber in the group bonus. One of the objectives that **Barclays** (2020 ARA, p122) linked the CEO's performance

to specifically references cyber: 'Oversee the effective management of the risk and controls agenda, including cyber risks'.

However, as noted by the European Union Agency for Cybersecurity, the level of threat is steadily increasing. The increasing sophistication of cyber attacks, their diverse sources and differing motivations ranging from making a political point, organised criminals wanting to profit financially, or nation states seeking intelligence and/or disruption, have been further exacerbated by the pandemic, which has forced business to become even more reliant on digital technology due to remote working.

It is therefore not surprising that of those companies in our sample that included cyber as a principal risk, 45% explicitly stated that the risk had increased in the year for the reasons above and reflecting the expectations that cyber regulations are likely to expand, given the growing focus from regulators in the UK, the EU and the US.

#### Changes to governance over cyber security

As the sophistication of attacks increases, so do the business impacts. Very often organisations refer to significant financial losses, major business disruption, the inability to

operate, loss of data, reputational damages and regulatory penalties or sanctions. This might explain why some companies like **Melrose Industries** (2020 ARA, p103) have opted to retain cyber risk oversight at the board level.

Given however that the role of the AC in reviewing the company's internal control and risk management systems encompasses assessing whether these are effective in preventing and detecting major cyber security incidents, most commonly it is the AC that has oversight over cyber resilience.

In light of the potential for a significant increase to AC responsibilities arising from the BEIS consultation, in conjunction with the rising cyber threats, boards may need to challenge whether the AC continues to have the bandwidth and support necessary to adequately oversee cyber risks, or whether these governance arrangements will need to evolve. Some companies are already reconsidering their governance over cyber security, with this trend being more prevalent within financial services, given the higher exposure of this industry to significant disruption from cyber attacks and regulator expectations.<sup>22</sup>

**Prudential** (2020 ARA, pp62, 99 and 152) during 2020 continued to work to operationalise the revised organisational structure and governance model for cyber security management. This change has resulted in a centralised Group-wide Information Security and Privacy function at management level which defines and provides governance and the risk management framework for information security risks across the Group. This Committee is a sub-committee of the Group Executive Risk Committee (GERC), chaired by

“  
The sophistication of threat capabilities increased in 2019, with many adversaries using exploits, credential stealing and multistage attacks

European Union Agency for Cybersecurity,  
The Year in Review, From January 2019 to April 2020

<sup>20</sup> The 2020 RBC Global Asset Management Responsible Investment Survey was conducted from June 16, 2020, through July 30, 2020, reflects the views of institutional investors and consultants from the US, Canada, Europe, and Asia (mainly Japan). The US accounted for over half (55%) of responses followed by Canada (23%), Europe (13%) and Asia (5%). In total, the survey reflects responses from 809 survey participants.

<sup>21</sup> **Cyber Security Breaches Survey 2021, Gov. UK, March 2021.**

<sup>22</sup> In 2017 the FCA, in its “**Good cyber security – the foundations**” guidance document, explicitly stated that under Principle 11 of the FCA Handbook, it expects companies to report material cyber incidents. More recently, FCA, Bank of England and the Prudential Regulation Authority (PRA) published a shared policy summary on new operational resilience requirements. By 31 March 2022 firms subject to these rules will need to, amongst others, have conducted lessons learnt exercises to ‘identify, prioritise, and invest in the firm's ability to respond and recover from disruptions as effectively as possible’ and developed internal and external communications plans for when important business services are disrupted. This will have to address cyber attack-related disruption.

the Group Chief Risk and Compliance Officer. As a standing member of the GERC, the Group Chief Information Security Officer (CISO) provides regular updates to the GERC and the Group Risk Committee on the cyber threats facing Prudential and the progress of Prudential's security programme. On a half-yearly basis, the Group CISO also holds a dedicated session with the Group Risk Committee to enable a more in-depth discussion on the cyber risk facing Prudential. The AC also play its role on cyber oversight: two joint meetings were held with the Risk Committee in May to discuss cyber security.

Some companies have created specific board committees separate from the AC. **Legal & General Group** (2020 ARA, p74) has set up a separate Technology Committee which focuses primarily on the company's IT, digital and cyber strategies and their implementation plans.

Others have set up advisory panels or working groups at management level to support the Board, AC or the Risk Committee. The **HSBC** board (HSBC 2020 ARA, pp204 and 227) approved the establishment of a

Technology Governance Working Group for a period of 12 months. The working group has been tasked with developing recommendations to strengthen the Board's oversight of technology strategy, governance and emerging risks and enhance connectivity with the principal subsidiaries. On the other hand, the approach to governance of technology risk and Cloud adoption has been one of the principal activities considered by the Group Risk Committee.

Similarly, **St. James's Place** (2020 ARA, p117) recognise that the importance of cyber and technology skills and experience has increased considerably in recent years. The Board agreed that this is an area where further expertise was required. The Nomination Committee did not believe it was prudent to place the responsibility for oversight with an individual director. Instead it concluded that it would be more appropriate to retain the oversight of cyber risks at the Board level and establish a Technology Advisory Group that could advise and educate them and keep it abreast of the latest developments on cyber and technology.

Regardless of the structure adopted, the board needs to be confident that the internal controls are appropriate and effective to detect and prevent major cyber security incidents. Effective risk management is not just the result of an effective AC or a separate, new committee but the result of multiple layers of risks defence. Crucial to this is the appropriate resourcing and funding of second line of defence functions – which provides more immediate and embedded assurance, instead of relying too heavily on third line of defence functions such as internal audit, which can sometimes be more backward looking. The chosen approach could be one of the topics covered by the A&A policy.

#### Prevent, detect and respond

No business is immune to cyber attacks which is why companies need to be prepared not only to prevent, but also to detect and respond.

As expected in the context of this being a principal risk, most companies set out in their ARA how they seek to mitigate cyber security risks. Very often companies refer to external cyber security maturity assessments, employee training or re-assessment of the internal

audit programmes to include cyber security. Some have enhanced their internal controls systems, have adopted recognised cyber schemes (e.g., UK Cyber Essentials<sup>23</sup>) or have opted to base their cyber security approach on recognised frameworks (e.g., the US National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) or Information Control Objectives and Technologies to Others<sup>24</sup> (COBIT)).

However, the explanation of the AC's oversight is typically covered off as part of the broader internal controls monitoring narrative, without specific reference to cyber. Better reporting includes outlining high level activities (e.g., receiving regular updates on cyber security risks/progress on implementation of IT platforms, reviewing the company's cyber security plan/cyber security strategy). One exception is **Mondi** (see **Figure 2.12**), whose ARA provides insight on the activities undertaken to oversee cyber as well as the frequency of the assessment. The report expressly states the result of the assessment '*Overall the committee concluded that the Group's IT risk management was effective, and that management ensured that it was subject to continuous monitoring and improvement*'.

While the methods mentioned above may help reduce cyber risks, it is abundantly clear that none of these methods can successfully prevent all cyber attacks; at the end of the day a maturity assessment<sup>25</sup> can only identify weaknesses in a company's cyber security defence and highlight the areas that need to be prioritised but it can never entirely eliminate the risk.

It is therefore not sufficient for boards to have confidence in the strength of preventative controls but also importantly in the business's

ability to respond and recover when an attack happens. In order for a company to be prepared for an attack from a crisis management perspective, it is crucial for the board to conduct a number of pervasive attack simulations and arrive at a set of planned responses that can be immediately drawn upon, at least as a starting point. We consider that this approach will become even more important for financial services firms under the new operational resilience requirements effective from 31 March 2022.

Despite the need to run attack simulations to maximise resilience and the fact that the majority of companies in our sample reported a cyber security related principal risk, only 12% of companies explicitly referenced cyber risk in their viability statement scenarios with a further 6% making no more than a high level reference to cyber. This might suggest that boards are not conducting sufficiently

severe cyber attack simulations, or if they are, these are not being fully translated into implications on viability.

We therefore recommend that when the AC challenges management's viability assessment (see **section 2.5.1**) it gives due consideration to whether the experiences from cyber simulations have been adequately reflected and considers the variety of metrics on cyber (e.g., the number of security incidents and their severity, their impact and the resolution state). For example, **National Grid** (2021 ARA, pp28-29) has a significant terror-related cyber attack taking place as its first viability scenario. Additionally, its risk cluster testing scenario involves a significant cyber attack, resulting in a significant data breach and a catastrophic asset failure, causing a significant disruption of energy supply, leading to loss of operator licence for one of the businesses.

#### Disclosing measures to mitigate cyber security risks

**Network International Holdings** (2020 ARA, p116) external maturity assessment conducted.

**Fresnillo** (2020 ARA, p123) cyber security approach is based on two frameworks: NIST CSF and COBIT.

**Derwent London** (2020 ARA, p144) renewed its UK Cyber Essentials accreditation.

**Synthomer** (2020 ARA, p91) reassessed priorities for internal audit and increased the focus on the resilience of its cyber security and business continuity plans.

**RHI Magnesita** (see **Figure 2.10**) enhanced IT security controls to address increased cyber security risk.

**Vesuvius** (2020 ARA, p32) has a plan in place to strengthen Vesuvius' overall IT security which is continually adapted as new risks emerge.

**Senior** (2020 ARA, p36) required all employees to complete online cyber/information security training and ran a campaign of cyber newsletters and posters to alert employees to cyber threats.

<sup>23</sup> **Cyber Essentials** is a UK Government backed scheme supported by the NCSC (National Cyber Security Centre) designed to help organisations of any size to protect themselves against the threat of cyber attacks.

<sup>24</sup> **NIST CSF** is voluntary guidance, based on existing standards, guidelines and practices for organisations to better manage and reduce cyber security risk. COBIT is an IT management framework developed by the Information Systems Audit and Control Association (ISACA) to help businesses develop, organise and implement strategies around information management and governance.

<sup>25</sup> The **National Cyber Security Centre** defines maturity models in cyber security as a 'tool for assessing an organisation's effectiveness at achieving a particular goal. They enable organisations to identify where their practices are weak or not taken seriously and where their practices are truly embedded'. In the context of cyber security, a maturity model gives an organisation's leadership a way to measure the progress made in embedding security into its day-to-day and strategic operations.

## 2.6 Metrics and targets

### 2.6.1 Audit quality

The BEIS consultation proposes that ARGA should impose additional requirements on ACs to continuously monitor audit quality, and consistently demand challenge and scepticism from auditors. There isn't much detail beyond this including what such continuous monitoring involves. If this is finalised, we expect that the current obligation in the Code for ACs "to review the effectiveness of the external audit process" will need to be amended to include specific reference to audit quality – this has better grounding in auditing standards, compared to the concept of effectiveness, which is very subjective.

#### Extract from FRC's Audit Quality Practice Aid for ACs (December 2019)

3.4 A high-quality audit provides investors and other stakeholders with a high level of assurance that the financial statements of an entity give a true and fair view and provide a reliable and trustworthy basis for taking decisions (or results in an auditor's report that sets out the basis for any disagreement with management or restriction on the ability of the auditor to give an opinion).

3.5 Auditors carrying out high-quality audit act with integrity and objectivity, are demonstrably independent and do not act in a way that risks compromising stakeholders' perceptions of that independence. A high-quality audit complies with both the spirit and the letter of regulation and is supported

In its 2015 publication, updated in 2019, the FRC noted that many AC members suggested that it was relatively straightforward to assess service levels in the external audit process, but less so to assess audit quality. The aid highlighted factors that ACs may consider when making their assessment of the quality of their external audit and hence the effectiveness of the external audit.

Participants at our FTSE 100 AC roundtable noted that they already had a robust dialogue with their auditor and considered audit quality to be the main criterion for auditor appointment and evaluation.

by rigorous due process and quality assurance. It clearly demonstrates how it reflects investor and other stakeholder expectations, is driven by a robust risk assessment informed by a thorough understanding of the entity and its environment, and provides challenge, transparency and insight in a clear and unambiguous way. High-quality audit also provides a strong deterrent effect against actions that may not be in the public interest, underpins stakeholder confidence, and drives continuous improvement.

3.27 Evaluation of audit quality entails assessing four key elements:

1. Mindset and culture
2. Skills, character and knowledge
3. Quality control
4. Judgment

The consultation indicates that ARGA will develop standards by which audit quality will be measured. Before these are formalised, ACs may find it helpful to use EY's practical toolkit for assessing the quality and effectiveness of external audit<sup>26</sup>, which reflects not only the FRC's aid, but also other international best practice guides. ACs may also want to consider what they could do to monitor audit quality on a continuous basis. One way could be through the use of regularly reviewed Audit Quality Indicators (AQIs) such as those suggested by the FRC in a recent Thematic Review.<sup>27</sup>

- ▶ Planned hours versus actual hours by grade: This is a metric that ACs may find useful to review on a regular basis as a proxy to gauge whether the total expected audit effort is being expended as the audit progresses, the involvement by senior team members in reviews and coaching etc., and allow the AC to intervene if the variances are material.
- ▶ Timeliness of the completion of key phases of the audit: Audits that meet milestones on a timely basis tend to be better planned, managed and controlled and therefore of a higher quality. Significant delays against milestones would again allow for timely AC intervention.

Given the various proposals to redefine the scope and purpose of the audit and its conduct, further metrics and indicators may become relevant in due course.

ACs will also need to consider what indicators could precipitate an external audit tender ahead of the regular ten-year cycle and potentially discuss this as part of

the A&A policy. This could be on the basis of unsatisfactory outcomes of continuous audit quality monitoring, or, as in the case of **Rentokil** (2020 ARA, p104), to evaluate whether audit requirements could be met in a different way in light of the group's changing size and shape, as well as technological developments in auditing software.

### 2.6.2 Performance, risks and internal controls

As data processing and analytics capabilities evolve, ACs need to challenge whether the reporting they get from management could be more insightful and decision-useful.

Tools, such as EY's Advanced Financial Analytics (AFA), help connect data not only from multiple internal sources but also from third-party sources including news, social media and macro-economic markets data providers. Such intelligent, real-time analytics in the form of dashboards are increasingly used by management to monitor business performance. Bespoke performance dashboards can also be created for directors, supplemented with commentary from management on key areas of change and investigation as a result of prior AC challenge.

Key risk indicators (KRIs) i.e., measures to understand or predict the level of risk a business is exposed to, are another source of information that can help the AC discharge of its duties. **Fresnillo** (2020 ARA, pp114-125) discloses KRIs monitored by the AC alongside its principal risk narrative. The business integrity function of **WPP** (2020 ARA, p93) is designing and building a risk analytics platform which will sit over dynamic data feeds and alongside refreshed risk appetite statements,

drivers and tolerances, incorporating **WPP's** internal control framework. The resulting dashboard analysis will allow risks to be monitored and tracked across all businesses and markets and will feed into the regular risk discussions of executive management, the AC and the Board.

As discussed in **section 2.3.3** management can also use dashboards to continuously monitor controls and therefore identify problems as they arise – which in turn speeds up remediation and impact on the overall control environment. ACs

may also consider the use of such dashboards to summarise internal controls assessments. During the COVID-19 pandemic **M&G** (2020 ARA, p104) produced a monthly Critical Controls Dashboard to provide its board with comfort over the control environment by monitoring the key risks and operation of the key controls impacted with input from all three lines of defence.



Fundamentally, risk management is about providing the business with robust risk insights to inform strategic decisions. Identification of emerging risks is not so much about predicting futuristic risks, but considering how key disruptive trends may interact in various combinations to create new challenges or opportunities for an organisation. Once this is understood, companies need to determine what signals — both internal and external — should be tracked to provide greater insight into the emergence and clarification of these trends and therefore the plausible impacts these may have.

The majority of the engagements we are currently working on with companies are focused on enhancing identification of emerging risks and predictive risk indicators to better inform decisions, but also with the aim of bringing together disparate sources of business data whilst applying a risk lens to tell the business something it doesn't already know. Tracking internal and external signals of change and reporting on this to the board is becoming a vitally important aspect of considering organisational resilience.

Emma Price, EY Associate Partner, Business Consulting  
[EPrice1@uk.ey.com](mailto:EPrice1@uk.ey.com)

<sup>26</sup> Assessing the quality and effectiveness of the external audit, A practical tool for audit committees, EY, April 2020.  
<sup>27</sup> Audit quality indicators, AQR thematic review, FRC, May 2020.

One of the BEIS proposals is for the regulator to have the power to place an observer on ACs if necessary.

Interview with Amarjit Singh, Partner at EY, heading up EY's Extended Assurance offerings to Wealth & Asset Management sector.



Amarjit Singh,  
EY Partner, Financial Services,  
[asingh@uk.ey.com](mailto:asingh@uk.ey.com)

1

**In what circumstances does the Prudential Regulatory Authority (PRA) exercise its power to place an observer on the AC?**

The PRA generally conducts yearly evaluation visits to regulated entities. During such visits, the PRA will be looking at a company's risk framework and may choose to attend the AC to enhance its understanding of this framework. The PRA will also inspect meeting minutes and other documents. If anything they see gives them cause for serious concern about the quality of governance, they may use their powers under section 166 of the Financial Services and Markets Act to appoint a "skilled person" to investigate the matter. But what is important to clarify is that a skilled person is not appointed to observe the AC. Rather the skilled person is appointed to investigate the PRA's concerns and that investigation may require attendance at the AC.

2

**Can you talk me through how this works in practice?**

Let's say that during its evaluation visit, the PRA notes from updates provided by IA that it is significantly behind plan. Nothing in the AC minutes suggests that additional resource will be allocated to allow them to catch up or even that the committee members consider the situation worrying. This raises concerns about IA effectiveness and the PRA may then request the firm appoint a skilled person specifically to assess this effectiveness. If the PRA appointed me as a skilled person, I would review IA reporting and the AC minutes from previous meetings. I would also speak to various individuals and with all this context in mind, attend the AC. When I attend the AC it is with the specific purpose of assessing IA effectiveness – I observe how IA interacts with management, with the AC, I take note of the styles, the personalities, the challenges that are being raised, the support that is being offered, how findings are received and recommendations acted upon. My role as an observer (at the AC or management meetings) is limited to the specific topic – I have to be very careful not to go outside the remit of my appointment.

3

**Given the BEIS proposals for ARGAs to have the power to appoint an observer on ACs if necessary, any final thoughts for AC members given you have been appointed as an observer?**

Any such investigation by the regulator is a serious matter – if the PRA concludes that it is not satisfied with the governance then in it may issue incremental capital guidance, requiring the firm to hold more capital to mitigate the risk associated with poor governance practice. But when the AC is being observed, it is not about the words or nit-picking; when I or the PRA attends the AC it is very much about getting a feeling for the culture – does the Chair chair appropriately? Are the topics that really matter being discussed? Are points raised not being dismissed? Are conversations being shut down or are views actively sought? Is the conversation balanced? Are decisions a done deal even before the debate starts? It is the softer side that we want to observe – the factual points we can read in the minutes!

Now of course, when people know you are coming, they will change their behaviours; there is no doubt about that. But an experienced skilled person, in the same way as an experienced external board evaluator, picks up pretty quickly on behaviours that are not authentic. We do not get fooled that easily!

## 2.7 Ten key questions to assess effectiveness

1

Aside from meeting the composition requirements of the Code and DTR is the AC considering and preparing for the future skills it will need for example, in light of changing circumstances of the company, its business model and the sector it operates in?

5

Are the number of meetings and time allocated to agenda items sufficient to discharge the AC's responsibilities?

9

Is there a structured process in place to assess the audit quality on a continuous/in-flight basis with appropriate reference to audit quality indicators?

2

Do the AC's terms of reference reflect not just the mandatory responsibilities as specified in regulations and Codes, but also the de facto ones, as well as the interaction between the AC and other committees?

6

Is the AC pack distributed with sufficient notice to allow the AC members to read and analyse the content and therefore have action-oriented meetings?

10

Does the AC report in the ARA present a fair picture of the activities of the AC, including challenges raised and their resolution?

3

Where there are separate risk and ACs, is the division of responsibilities between the two clearly defined?

7

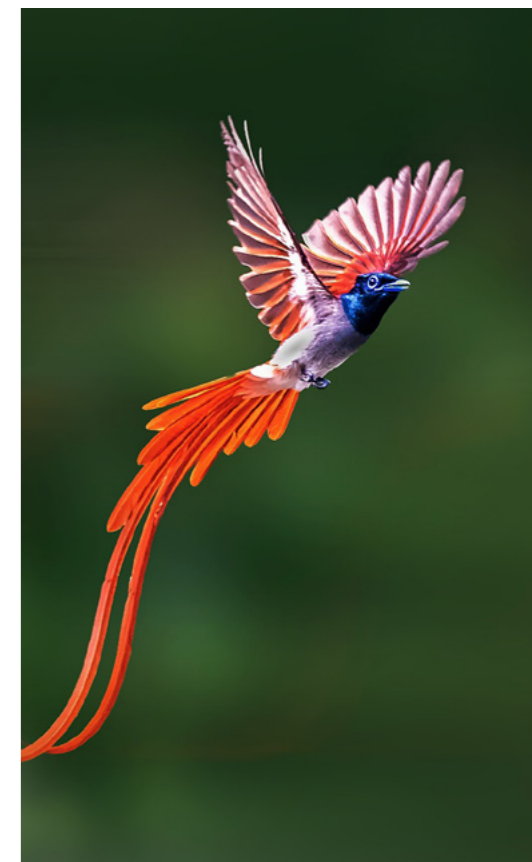
Is the documentation provided by management to the AC of sufficient detail and quality to allow the AC to challenge management's views? Is the AC's review and challenge of this documentation adequately minuted to withstand future regulatory scrutiny?

4

Is there an effective induction programme for new members and on-going training thereafter?

8

Does the AC have a complete and accurate picture of the existing assurance landscape and how this compares to the expectations of the board and external stakeholders?



2.8 Reporting examples

Figure 2.1  
Smith + Nephew: Details on the system of internal control over financial reporting (2020 ARA, pp96 and 97)

<p><b>Evaluation of internal controls</b></p> <p>Management is responsible for establishing and maintaining adequate internal control over financial reporting as defined in Rule 13a–15(f) and 15d–15(f) under the US Securities Exchange Act of 1934.</p> <p>There is an established system of internal control throughout the Group and our country business units. The main elements of the internal control framework are:</p> <ul style="list-style-type: none"><li>– The management of each country and Group function is responsible for the establishment, maintenance and review of effective financial controls within their business unit or function.</li><li>– The Group's IT organisation is responsible for the establishment of effective IT controls within the core financial systems and underlying IT infrastructure.</li><li>– The Financial Controls &amp; Compliance Group has responsibility for the review of the effectiveness of controls operating in the countries, functions and IT organisation, either by performing testing directly; reviewing testing performed in-country; or utilising a qualified third party to perform this management testing on its behalf.</li><li>– The Group Finance Manual sets out financial and accounting policies, and is updated regularly. The Group's Minimum Acceptable Practices (MAPs) were updated in 2020 with a new manual. The business is required to self-assess their level of compliance with the MAPs on a regular basis and remediate any gaps.</li><li>– MAPs compliance is validated through spot-checks conducted by the Financial Controls &amp; Compliance Group and during both Internal Audit and external audit visits. The technology solution to facilitate the real time monitoring of the operation and testing of controls has been partially implemented in 2020 and this will be completed in 2021.</li><li>– There are clearly defined lines of accountability and delegations of authority.</li><li>– The Internal Audit function executes a risk-based annual work plan, as approved by the Audit Committee.</li><li>– The Audit Committee reviews reports from Internal Audit on their findings on internal financial controls, including compliance with MAPs and from the SVP Group Finance and the heads of the Financial Controls &amp; Compliance, Taxation and Treasury functions.</li></ul>	<ul style="list-style-type: none"><li>– The Audit Committee reviews regular reports from the Financial Controls &amp; Compliance Group with regard to compliance with the SoX Act including the scope and results of management's testing and progress regarding any remediation, as well as the aggregated results of MAPs self-assessments performed by the business.</li><li>– Business continuity planning, including preventative and contingency measures, back-up capabilities and the purchase of insurance.</li><li>– Risk management policies and procedures including segregation of duties, transaction authorisation, monitoring, financial and managerial review and comprehensive reporting and analysis against approved standards and budgets.</li><li>– A treasury operating framework and Group treasury team, accountable for all treasury activities, which establishes policies and manages liquidity and financial risks, including foreign exchange, interest rate and counterparty exposures. Treasury policies, risk limits and monitoring procedures are reviewed regularly by the Audit Committee, or the Finance &amp; Banking Committee, on behalf of the Board.</li><li>– Our published Group tax strategy which details our approach to tax risk management and governance, tax compliance, tax planning, the level of tax risk we are prepared to accept and how we deal with tax authorities, which is reviewed by the Audit Committee on behalf of the Board.</li><li>– The Audit Committee reviews the Group whistle-blower procedures to ensure they are effective.</li><li>– The Audit Committee continued to receive and review reports on the progress of the Finance Transformation element of the APEX programme during 2020 and the mitigation of the associated risks.</li></ul>	<p>This system of internal control has been designed to manage rather than eliminate material risks to the achievement of our strategic and business objectives and can provide only reasonable, and not absolute, assurance against material misstatement or loss. Because of inherent limitation, our internal controls over financial reporting may not prevent or detect all misstatements. In addition, our projections of any evaluation of effectiveness in future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate. Entities where the Company does not hold a controlling interest have their own processes of internal controls.</p> <p>We have reviewed the system of internal financial control and satisfied ourselves that we are meeting the required standards both for the year ended 31 December 2020 and up to the date of approval of this Annual Report. No concerns were raised with us in 2020 regarding possible improprieties in matters of financial reporting.</p> <p>This process complies with the FRC's 'Guidance on Risk Management, Internal Control and Related Financial and Business Reporting' under the UK Corporate Governance Code and additionally contributes to our compliance with the obligations under the SoX Act and other internal assurance activities. There has been no change during the period covered by this Annual Report that has materially affected, or is reasonably likely to materially affect, the Group's internal control over financial reporting.</p> <p>The Board is responsible overall for reviewing and approving the adequacy and effectiveness of the risk management framework and the system of internal controls over financial, operational (including quality management and ethical compliance) processes operated by the Group. The Board has delegated responsibility for this review to the Audit Committee. The Audit Committee, through its Internal Audit function, reviews the adequacy and effectiveness of internal control procedures and identifies any significant weaknesses and ensures these are remediated within agreed timelines. The latest review covered the financial</p>	<p>year to 31 December 2020 and included the period up to the approval of this Annual Report. The main elements of this review are as follows:</p> <ul style="list-style-type: none"><li>– The Chief Executive Officer and the Chief Financial Officer evaluated the effectiveness of the design and operation of the Group's disclosure controls and procedures as at 31 December 2020. Based upon the evaluation, the Chief Executive Officer and Chief Financial Officer concluded on 18 February 2021 that the disclosure controls and procedures were effective as at 31 December 2020.</li><li>– Management is responsible for establishing and maintaining adequate internal control over financial reporting. Management assessed the effectiveness of the Group's internal control over financial reporting as at 31 December 2020 in accordance with the requirements in the US under section 404 of the SoX Act. In making that assessment, they used the criteria set forth by the Committee of Sponsoring Organisations of the Treadway Commission in Internal Control-Integrated Framework (2013). Based on their assessment, management concluded and reported that, as at 31 December 2020, the Group's internal control over financial reporting was effective based on those criteria. Having received the report from management, the Audit Committee reports to the Board on the effectiveness of controls. KPMG, an independent registered public accounting firm, audited the financial statements included in the 2020 Annual Report, containing the disclosure required by this item, issued an attestation report on the Group's internal control over financial reporting as at 31 December 2020.</li></ul>	<table><tr><td><b>Internal controls</b></td></tr><tr><td><ul style="list-style-type: none"><li>– <b>Monitoring the effectiveness of internal controls and compliance with the UK Corporate Governance Code 2018 and the SoX Act, specifically sections 302 and 404.</b></li><li>– <b>Reviewing the operation of the Group's risk mitigation processes and the control environment over financial risk.</b></li></ul></td></tr><tr><td><b>Early February</b><ul style="list-style-type: none"><li>– Considered SoX 2019 audit process and MAPs update.</li></ul></td></tr><tr><td><b>Late February</b><ul style="list-style-type: none"><li>– Reviewed effectiveness of Internal Controls over financial reporting and SoX.</li><li>– Reviewed S302 and S906 certifications.</li></ul></td></tr><tr><td><b>April</b><ul style="list-style-type: none"><li>– Considered SoX and MAPs Planning for 2020 including S404 scope.</li></ul></td></tr><tr><td><b>July</b><ul style="list-style-type: none"><li>– Reviewed new process for the completion of SoX and MAPs year end work, including the impact of COVID-19.</li></ul></td></tr><tr><td><b>September</b><ul style="list-style-type: none"><li>– Considered SoX and MAPs progress.</li></ul></td></tr><tr><td><b>October</b><ul style="list-style-type: none"><li>– Reviewed update on IT controls.</li></ul></td></tr><tr><td><b>December</b><ul style="list-style-type: none"><li>– Considered SoX and MAPs progress, including the impact of COVID-19.</li></ul></td></tr><tr><td><b>Fraud &amp; whistle-blowing</b></td></tr><tr><td><ul style="list-style-type: none"><li>– <b>Receiving reports on the processes in place to prevent fraud and to enable whistle-blowing.</b></li><li>– <b>If significant, receive and review reports of potential fraud or whistle-blowing incidents. Reviewed Internal Audit report on fraud.</b></li></ul></td></tr><tr><td><b>Early February</b><ul style="list-style-type: none"><li>– Reviewed year end report, including fraud.</li></ul></td></tr></table>	<b>Internal controls</b>	<ul style="list-style-type: none"><li>– <b>Monitoring the effectiveness of internal controls and compliance with the UK Corporate Governance Code 2018 and the SoX Act, specifically sections 302 and 404.</b></li><li>– <b>Reviewing the operation of the Group's risk mitigation processes and the control environment over financial risk.</b></li></ul>	<b>Early February</b> <ul style="list-style-type: none"><li>– Considered SoX 2019 audit process and MAPs update.</li></ul>	<b>Late February</b> <ul style="list-style-type: none"><li>– Reviewed effectiveness of Internal Controls over financial reporting and SoX.</li><li>– Reviewed S302 and S906 certifications.</li></ul>	<b>April</b> <ul style="list-style-type: none"><li>– Considered SoX and MAPs Planning for 2020 including S404 scope.</li></ul>	<b>July</b> <ul style="list-style-type: none"><li>– Reviewed new process for the completion of SoX and MAPs year end work, including the impact of COVID-19.</li></ul>	<b>September</b> <ul style="list-style-type: none"><li>– Considered SoX and MAPs progress.</li></ul>	<b>October</b> <ul style="list-style-type: none"><li>– Reviewed update on IT controls.</li></ul>	<b>December</b> <ul style="list-style-type: none"><li>– Considered SoX and MAPs progress, including the impact of COVID-19.</li></ul>	<b>Fraud &amp; whistle-blowing</b>	<ul style="list-style-type: none"><li>– <b>Receiving reports on the processes in place to prevent fraud and to enable whistle-blowing.</b></li><li>– <b>If significant, receive and review reports of potential fraud or whistle-blowing incidents. Reviewed Internal Audit report on fraud.</b></li></ul>	<b>Early February</b> <ul style="list-style-type: none"><li>– Reviewed year end report, including fraud.</li></ul>
<b>Internal controls</b>																
<ul style="list-style-type: none"><li>– <b>Monitoring the effectiveness of internal controls and compliance with the UK Corporate Governance Code 2018 and the SoX Act, specifically sections 302 and 404.</b></li><li>– <b>Reviewing the operation of the Group's risk mitigation processes and the control environment over financial risk.</b></li></ul>																
<b>Early February</b> <ul style="list-style-type: none"><li>– Considered SoX 2019 audit process and MAPs update.</li></ul>																
<b>Late February</b> <ul style="list-style-type: none"><li>– Reviewed effectiveness of Internal Controls over financial reporting and SoX.</li><li>– Reviewed S302 and S906 certifications.</li></ul>																
<b>April</b> <ul style="list-style-type: none"><li>– Considered SoX and MAPs Planning for 2020 including S404 scope.</li></ul>																
<b>July</b> <ul style="list-style-type: none"><li>– Reviewed new process for the completion of SoX and MAPs year end work, including the impact of COVID-19.</li></ul>																
<b>September</b> <ul style="list-style-type: none"><li>– Considered SoX and MAPs progress.</li></ul>																
<b>October</b> <ul style="list-style-type: none"><li>– Reviewed update on IT controls.</li></ul>																
<b>December</b> <ul style="list-style-type: none"><li>– Considered SoX and MAPs progress, including the impact of COVID-19.</li></ul>																
<b>Fraud &amp; whistle-blowing</b>																
<ul style="list-style-type: none"><li>– <b>Receiving reports on the processes in place to prevent fraud and to enable whistle-blowing.</b></li><li>– <b>If significant, receive and review reports of potential fraud or whistle-blowing incidents. Reviewed Internal Audit report on fraud.</b></li></ul>																
<b>Early February</b> <ul style="list-style-type: none"><li>– Reviewed year end report, including fraud.</li></ul>																

**Figure 2.2**  
Capita: Finance transformation and improvement initiatives regarding internal controls over financial reporting (2020 ARA, pp52 and 53)

**Improvement initiatives**

The ARC has previously reported on the multiple initiatives launched to develop the risk management approach which is based on a three lines of defence model.

As the transformation of Capita has progressed, it has become evident that continued focus on our people, culture, systems, processes and controls is required – to drive greater awareness and consistency in how we identify, manage and mitigate risks. The key features are set out below:

- The risk management process was redefined in 2019 with an enhanced focus on:
  - Risk environment.
  - Risk assessment, response, and mitigation actions.
  - Monitoring and reporting.
- the Group executive risk committee (ERC) was established to oversee and challenge the key business risks and compliance activities.
- a specific financial services risk committee was reconstituted in 2019 to provide oversight of the regulated and financial services businesses within Capita.
- the Group embarked on an update to the enterprise risk management framework (ERMF), and a comprehensive control risk self-assessment (CRSA) tool was developed and piloted in 2019.
- the Group embarked on a finance transformation programme to drive improved data quality and standardisation of activities performed by the finance community. This has included an evaluation of financial controls by the senior finance team to review the material financial controls in place for effectiveness. The finance transformation will be supported in the future by the introduction of a new accounting system.

The above initiatives were further advanced in 2020, supported by the following key activities:

- A key control questionnaire (KCQ) process was developed and completed which identified key entity level controls across 14 Group wide areas. Every business leader was required to attest compliance with key controls within their functional, divisional, and business areas.
- Across the finance teams, the annual control questionnaire process was enhanced and completed where every business leader attested to compliance with a set of key financial controls.

- Senior management provided an assessment of the control environment following a stabilising of the initial pandemic crisis; specific attention was given to the plans to improve cyber and IT resilience.

The next stage of the improvement plan will be ensuring that the responses to the KCQ are developed and evidenced, such that the responses can then be subject to independent assurance.

**Internal controls**

A KCQ process was developed and completed during 2020. The results serve as a baseline for improvement and while there have been notable improvements in the control environment in recent years, eg bid reviews, there is still improvement to be made. The process helped verify known control weaknesses in IT resilience and cyber security. These weaknesses are, and will continue to be, addressed at a Group and division/function level by implementing effective corrective measures.

During 2020, a Group accounting policy manual and, for some areas, newly developed standard ways of working have been issued. A financial control tool was developed during the year to document existing key control detail at a business unit level and link to standard ways of working as they continue to be developed. Actions to improve compliance with key financial controls are logged and tracked through the tool. The process of identifying and documenting the key controls is further supported by necessary assurances from divisional management.

During 2021, further work will be taken to improve elements of our control framework. Action plans supported with investment to address some of the IT resilience and cyber security weaknesses are in place. Work will also continue to further enhance certain elements of the financial control framework. As we restructure our business, we will clarify the accountability, responsibility and strengthen our three lines of defence model, including maturing our internal control framework. The executive risk committee will provide oversight of these activities.

**Figure 2.3**  
Howden Joinery Group: Clarifying key controls (2020 ARA, p133)

**Controls and internal audit**

**Internal control framework**

The Group has an established framework of internal controls, which includes the following key elements:

- The Board approves the Group's strategy and annual budgets; the Executive Committee are accountable for performance within these.
- The Group and its subsidiaries operate control procedures designed to ensure complete and accurate accounting of financial transactions and to limit exposure to loss of assets or fraud.
- The Audit Committee meets regularly and its responsibilities are set out in the Audit Committee Terms of Reference (which may be found on the Company's website at [www.howdenjoinerygroupplc.com/governance/corporate-governance-report/terms-of-reference-of-the-audit-committee](http://www.howdenjoinerygroupplc.com/governance/corporate-governance-report/terms-of-reference-of-the-audit-committee)). It receives reports from the Internal Audit function on the results of work carried out under an annually agreed audit programme. Operational and compliance controls are considered when the Committee reviews the annual Internal Audit programme. The Audit Committee has full and unfettered access to the internal and external auditors.
- Operating entities provide certified statements of compliance with specified key financial controls. These controls are then cyclically tested by Internal Audit to ensure they remain effective, and are being consistently applied.
- The Audit Committee annually assesses the effectiveness of the assurance provided by the internal and external auditors. Every five years an external assessment is also undertaken with regard to the assurance provided by the Internal Audit department. An external assessment was undertaken by Grant Thornton in 2017.

A case study on the review of key controls may be found on page 133.

**Case study  
Key controls**

During 2020 we have worked to clarify our key controls across the business to focus and further strengthen our overall control framework. Sponsored by the CEO and CFO, and reporting regularly to the Audit Committee, this project is improving our capability to identify operational, IT and financial controls which mitigate our key and principal risks. Phase 1 of this project was delivered in 2020, with further phases starting in H1 2021.

Our project streams will reinforce key responsibilities across the business and their verification, assist new systems design, and enable us to address regulatory consequences of the Brydon and Kingman reviews when these are known. The immediate results include:

- A sustainable approach for cataloguing, monitoring and ownership of key controls.
- Embedding of operational ownership to measure effectiveness.
- An even stronger attestation process.

We see this exercise as both a necessity and an opportunity to further strengthen our control framework whilst protecting the essential Howdens locally empowered culture.

Working alongside the project, the Internal Audit team has embedded a new industry standard software solution that integrates enterprise risk assessments with independent control and audit activity. This solution has enabled further development of risk-based assurance and reporting capabilities, giving the Audit Committee, Board and Executive Committee a clearer view of control effectiveness.

**Figure 2.4**  
Unilever: Web page disclosure summarising approach to assurance

**Our approach to assurance**

We need accurate and robust data on our sustainability performance to help us make decisions, monitor performance and report progress to our stakeholders.

Our Environmental and Occupational Safety performance measures have been independently assured since 1996 by globally recognised providers. In 2011 we began to assure selected key performance measures in the Unilever Sustainable Living Plan (USLP). In 2020 we continued to attain limited assurance of selected Environmental and Occupational Safety performance indicators – see below for more details.

In addition to assurance of selected Environmental and Occupational Safety performance indicators noted above, we developed a phased assurance programme that enabled us to gain independent limited assurance over selected metrics in the USLP covering the nine pillars: Greenhouse Gas, Water, Waste & packaging, Sustainable sourcing, Health & hygiene, Nutrition, Fairness in the workplace, Opportunities for women and Inclusive business.

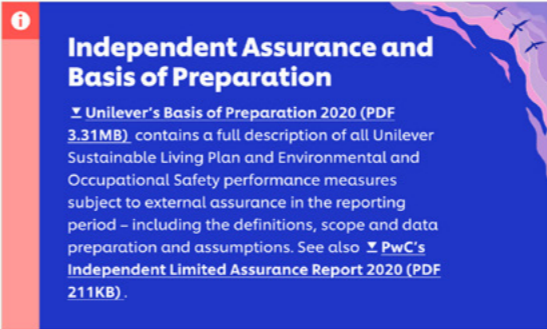
There are currently no industry norms or globally recognised practices for evaluating and measuring many of the performance indicators in the USLP. Furthermore, given the complexity of the USLP, we decided that annual assurance for every pillar each year was not practical. Over the course of the USLP, each pillar commitment has been assured at least twice – and in most cases more.

Our assurance plan is approved each year by the Board's Audit Committee.

**External assurance in 2020**

We reappointed PricewaterhouseCoopers LLP (PwC) to provide independent assurance for the ninth consecutive year. PwC's assurance engagement is in accordance with ISAE 3000 and they apply the Institute of Chartered Accountants in England & Wales (ICAEW) Code of Ethics. The Unilever Board's Audit Committee oversees the USLP assurance programme.

In 2020, PwC's scope was to provide limited assurance of selected Environmental and Occupational Safety performance measures and selected USLP pillar commitments: Health & Hygiene, Waste & Packaging, Fairness in the Workplace, Opportunities for Women, Nutrition and Sustainable Sourcing, as well as selected Inclusive Business metrics.



**Independent Assurance and Basis of Preparation**

Unilever's Basis of Preparation 2020 (PDF 3.31MB) contains a full description of all Unilever Sustainable Living Plan and Environmental and Occupational Safety performance measures subject to external assurance in the reporting period – including the definitions, scope and data preparation and assumptions. See also PwC's Independent Limited Assurance Report 2020 (PDF 211KB).

The environmental performance indicators assured were chosen because they reflect the main environmental aspects for our manufacturing sites, including utilities consumption, and waste, air and water pollution. Occupational safety indicators were chosen because safety at work is a top priority for our business.

**Ensuring rigorous reporting**

We have a number of processes to ensure that we publish information that is accurate and provides a transparent representation of our business.

The Unilever Compass includes a number of sustainability targets, many of which are ground-breaking in what they seek to measure. In 2016, we established the Metrics Team to provide strategic oversight of our metrics and to act as a decision-making body to ensure the ongoing rigour of our reporting. The Metrics Team includes representatives from Finance, Communications and Sustainability.

As well as setting principles for the development and governance of metrics, the Metrics Team ensures every metric has an owner who is a senior expert in the subject. This owner is responsible for understanding the activity underlying the metric (such as handwashing practices or sourcing of sustainable palm oil) and its efficient measurement, calculation and validation.

Each metric is supported by a Basis of Preparation (i.e. an explanation of how the data is collected and calculated and any assumptions made) to ensure a consistent approach year-on-year.

Our sustainability performance targets are tracked annually via a bespoke reporting solution known as ELMA (Electronic, Measurement, Analytics). ELMA has been configured to ensure data accuracy, such as electronic validation and algorithms to prevent double counting.

Our Finance team validates the result and supporting evidence in ELMA to ensure that calculation methods match the stated basis of preparation and that results are correctly aggregated and consistent with the previous year.

Figure 2.5  
ITV: Viability statement (2020 ARA, pp85 and 87)

Viability statement	
<p><b>How we assess prospects and risks</b></p> <p>The Board continually assesses ITV's prospects and risks at its meetings, including the following:</p> <ul style="list-style-type: none"><li>• Holding 'Strategy Days' twice a year, to oversee the delivery of the Strategy and consider changes to or new initiatives to further improve the ITV Strategy. Further detail can be found in the overview of Board meetings in 2020, from page 116</li><li>• Considering ad-hoc topics on strategic areas at the periodic Board meetings. Further detail can be found in the overview of Board meetings in 2020, from page 116</li><li>• Performing a full review of the principal and emerging risks twice a year. Further detail can be found earlier within the Principal Risks and Uncertainties section</li><li>• Performing periodic deep dives on specific risk areas, to further scrutinise the effectiveness of risk mitigation approaches and confirm operation within risk appetite. Further detail can be found earlier within the Principal Risks and Uncertainties section</li><li>• The Board and management significantly increased their focus on ITV's prospects, risks and viability in light of the evolving COVID-19 situation. This involved holding a session on the specific impact of COVID-19 on ITV's Strategy (June 2020); developing a range of COVID-19 scenarios for 2020 and beyond and modelling their potential financial impact; identifying cost interventions/mitigations to respond to severe downside scenarios; and increasing the level of financial performance reviews and reforecasting to track performance against these scenarios. Further details of the specific measures to respond to COVID-19 are provided in the Chief Executive's Report, page 14.</li></ul>	<p><b>How we assess viability</b></p> <p>When assessing the longer-term viability of ITV, we considered (i) ITV's strategy and business model (page 20 to 23); (ii) the principal risks and uncertainties (page 76 to 84); (iii) the Group's financing facilities, including covenant tests and future funding plans (page 60); (iv) the long range financial plan and cash forecast; and (v) other sensitivity factors or risks which have the potential to materially impact liquidity and cash in the assessment period.</p> <p>Based on this review a set of hypothetical and severe but plausible scenarios were developed. We then modelled these scenarios against the long-range financial plan and cash forecast both individually and in parallel, in order to assess viability.</p> <p>The output from this work was reviewed and approved by the Board and the Audit and Risk Committee. In reaching its view, the Board and Committee also considered analyst commentary, to understand the wider market and views on the Group's future prospects, and the external auditor's findings and conclusions on this matter. Further detail of the work performed by the Audit and Risk Committee to consider assumptions applied in the assessment viability is set out on page 118.</p>
<p><b>Assessment period for viability</b></p> <p>The Board reviewed the long range financial and strategic planning horizon and is of the view that a three year assessment period (1 January 2021 to 31 December 2023) continues to be most appropriate. The factors the Board considered in adopting this timeframe were as follows:</p> <ul style="list-style-type: none"><li>• The situation with respect to the COVID-19 pandemic remains uncertain and is likely to continue impacting ITV in the medium term. We are closely monitoring the external environment and continue to manage the risks associated with the pandemic to support us in returning to pre-COVID performance levels. Further detail of our response to COVID-19 is provided within the Chief Executive's Report, page 14 and in the COVID-19 principal risk mitigations, page 76</li><li>• Visibility over ITV's broadcast advertising business is relatively short term. Advertising remains cyclical and closely linked to the UK economic growth, which may continue to be impacted by the COVID-19 pandemic, Brexit and other uncertainties in the UK macroeconomic climate</li></ul>	<ul style="list-style-type: none"><li>• The commissioning process and life cycle of programming gives the ITV Studios division more medium-term outlook. However, while non-returning brands are replaced with new commissions, over time there is less visibility as programmes can experience changes in viewer demand or come to a natural expiration</li><li>• Technology and innovation in the media industry continues to change the demand for content and also how it is consumed</li><li>• Pension funding, which is one of ITV's key funding obligations, is agreed triennially with the Trustees of the pension schemes</li><li>• ITV's business model does not necessitate investment in large capital projects that would require a longer-term horizon assessment or returns</li></ul> <p><b>Assumptions applied</b></p> <p>We applied the following assumptions when assessing viability in the scenarios below:</p> <ul style="list-style-type: none"><li>• A vaccine is not rolled out to a substantial number of the population in territories in which we operate until the end of 2022, which delays businesses returning to normal operations</li></ul> <ul style="list-style-type: none"><li>• Consequently, there is the possibility of national and local lockdowns during this period</li><li>• Ongoing additional production costs associated with COVID-19 protocols and health and safety measures until the vaccine is rolled out</li><li>• Ongoing access to the UK bond market, but with an increased interest rate on bonds renewed in the period to reflect a potential decrease in credit rating</li><li>• Ongoing availability of the financing facilities, but at increased interest rates. This comprises of; an undrawn Revolving Credit Facility of £630 million expiring on 15 December 2023; and a bilateral financing facility of £300 million expiring in June 2026, of which £199 million is available as at 9 March 2021</li></ul>
<p>Taking into account current operational and financial performance, the Board has analysed the impact of following hypothetical scenarios. These scenarios were assessed in isolation and in parallel to further stress test viability:</p>	
<p>Scenario modelled</p>	<p>Link to Principal risks</p>
<p>Scenario 1</p>	
<p><b>A significant and sustained downturn in the advertising market when compared to 2019, as a result of further COVID-19 lockdowns, the possible impact of Brexit or other macro economic factors. In this scenario we also fail to replace the advertising revenue lost as a result of the government's announced restriction on HFSS advertising, which is due to come into force from the beginning of 2023.</b></p> <p>Based on our experiences during the initial 2020 COVID-19 lockdown the scenario assumes total advertising revenues continuing to remain significantly below 2019 level (2021 versus 2019: -9%); (2022 versus 2021: 1%*); (2023 versus 2022: -4%)</p> <p>1. *1% year-on-year increase, reflects marginal macroeconomic recovery in 2022 versus 2021, but still represents a significantly reduced position when compared to 2019. 2023 is further impacted by HFSS regulation.</p> <p><b>Business area impacted</b></p> <p>Broadcast (to become Media and Entertainment)</p>	<ul style="list-style-type: none"><li>• Advertising market changes</li><li>• Policy and regulatory changes</li><li>• COVID-19 pandemic</li><li>• Changing viewer habits</li></ul> <p>Further detail of how we are mitigating these risks are included in the earlier Risks and Uncertainties section</p>
<p>Scenario 2</p>	
<p><b>A number of key programme brands within the ITV Studios division are not recommissioned and new format growth does not materialise.</b></p> <p>Although 2021 would typically be too imminent for commissioners to make a decision to cancel a show, we have included the scenario from 2021 onwards to reflect ongoing risk of decreased production activity/delivery due to COVID-19. The scenario assumes key shows come to an end from 2021 (2021 impact: circa £45 million; 2022 and 2023 impact: circa £65 million p.a.)</p> <p><b>Business area impacted</b></p> <p>Studios</p>	<ul style="list-style-type: none"><li>• Evolving demand in the content market</li><li>• COVID-19 pandemic</li></ul> <p>Further detail of how we are mitigating these risks are included in the earlier Risks and Uncertainties section</p>
<p>Scenario modelled</p>	<p>Link to Principal risks</p>
<p>Scenario 3</p>	
<p><b>A significant change in ITV's pension funding obligations, following the triennial valuation in March 2021 resulting in a significant increase in pension deficit funding payments.</b></p> <p>This scenario assumes that pension funding payments increase from £75 million p.a. to £115 million p.a. in 2021 and remain flat in the following two years.</p> <p><b>Business area impacted</b></p> <p>Group</p>	<ul style="list-style-type: none"><li>• Pension deficit increases</li></ul> <p>Further detail of how we are mitigating these risks are included in the earlier Risks and Uncertainties section</p>
<p>Scenario modelled</p>	<p>Link to Accounting judgements and estimates</p>
<p>Scenario 4</p>	
<p><b>Settlements for ongoing litigation and earnouts for our larger acquisitions are significantly higher than estimated, resulting in large one-off cash payments.</b></p> <p>This scenario assumes increased acquisition earnout payouts in 2021 (see note 3.1.5 of the financial statements) and payments in 2023 (see note 4.3 of the financial statements).</p> <p><b>Business area impacted</b></p> <p>Group</p>	<ul style="list-style-type: none"><li>• The complexity and potential scale of the ongoing litigation settlements and earnout negotiations, results in a lack of certainty in the final liabilities and payments</li></ul> <p>Further detail of the accounting judgements and estimates applied to ongoing litigation and earnouts are provided in Section 1 of the Financial Statements. An overview the assessments performed by the Audit and Risk Committee with respect to these accounting judgements is provided on page 115 of the Audit and Risk Committee report</p>

Figure 2.6  
Reckitt: Risk interconnectivity (2020 ARA, p83)

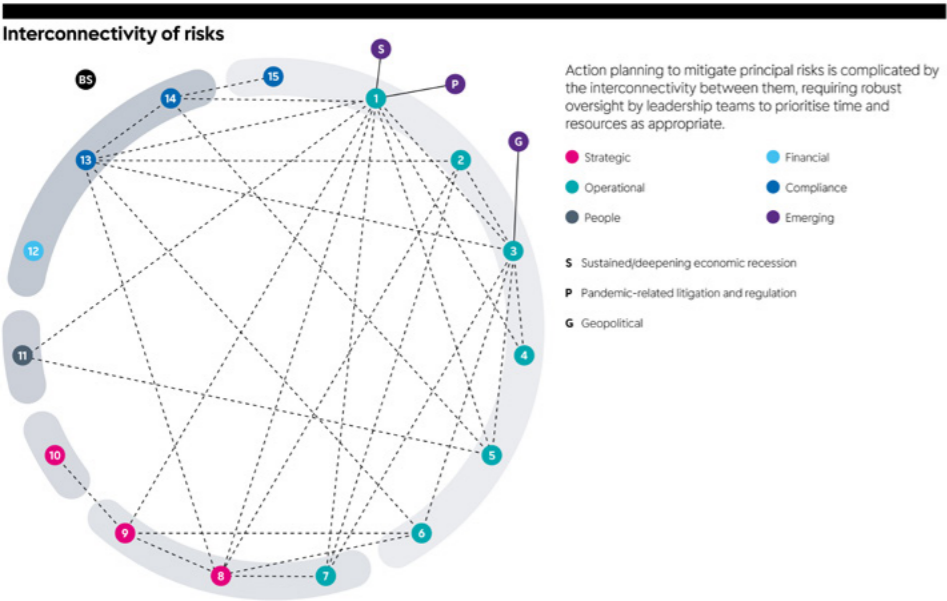
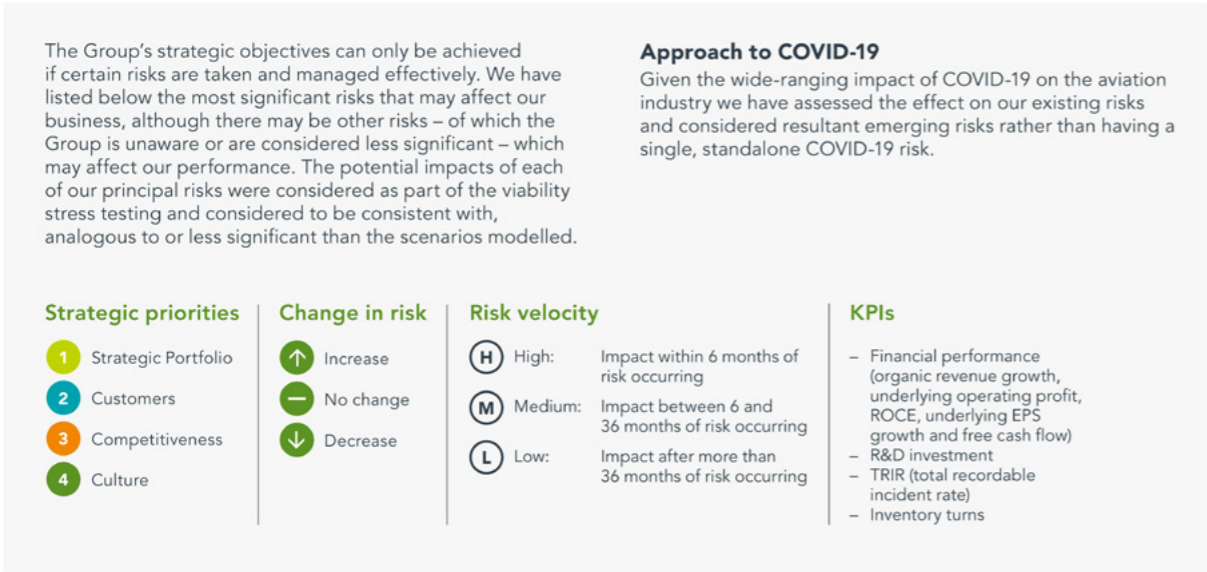


Figure 2.7  
Meggitt: Risk velocity (2020 ARA, p56)



Strategic risks

Risk	Description	Impact	How we manage it
<b>Industry changes</b> <div>1 ↑ H</div>	Significant variation in demand for air travel and/or our products due to aerospace and defence business downcycles coinciding; serious political, economic, pandemic (including the on-going impacts of COVID-19) or terrorist events; or industry consolidation that materially changes the competitive landscape.	Volatility in revenue and underlying profitability.	<ul style="list-style-type: none"><li>Demand is managed by monitoring external economic and commercial environment and long-lead indicators whilst maintaining focus on balanced portfolio.</li><li>Monitoring international political and tax developments to assess implications of future legislation.</li></ul>
<b>KPIs:</b> <ul style="list-style-type: none"><li>Financial performance</li></ul>			

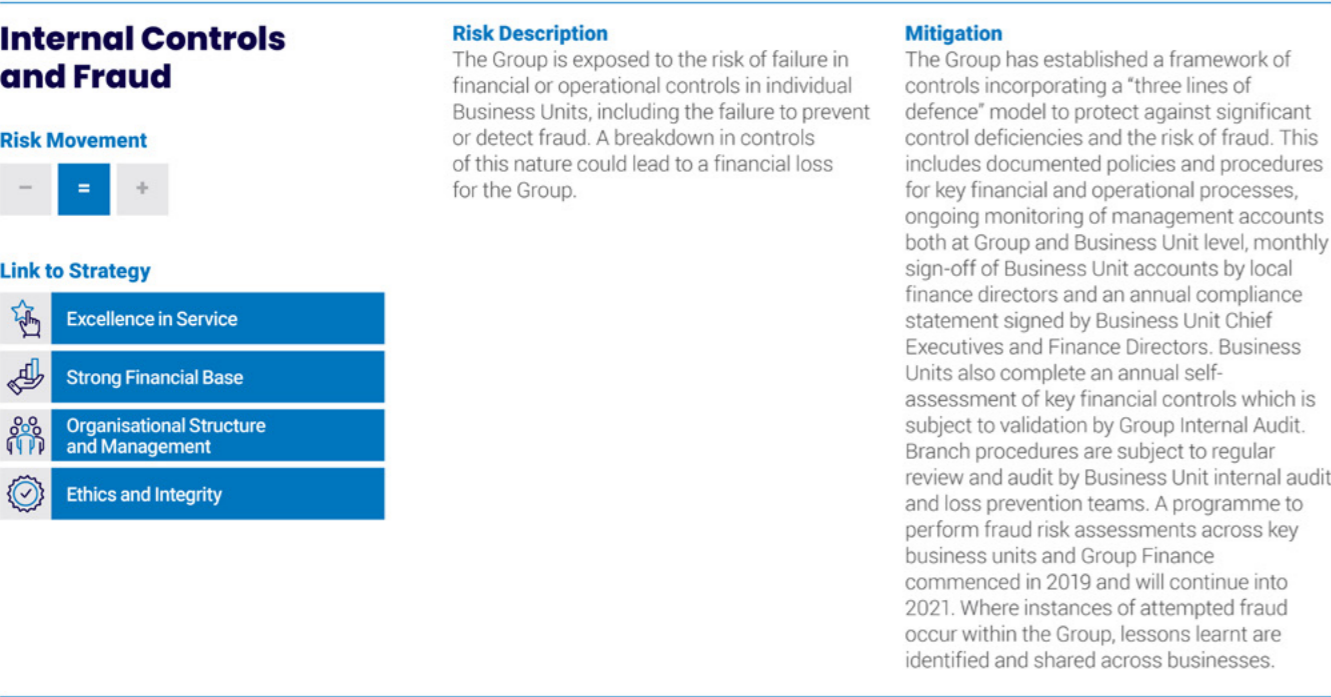
Figure 2.8  
St. James's Place: Resilience over different time horizons (2020 ARA, p80)

Over the next year	Over the next five years	Beyond 2025
<p><b>Risks</b></p> <p>The key risks to business resilience in the short term are likely to be operational in nature, such as data loss or increased cyber crime as a result of remote working. It is not expected that solvency will be an issue in the short-term due to our matching approach for client liabilities. Liquidity risks would be relevant for this time window since liquidity risks tend to be short-term in nature. However, we do not anticipate there being any liquidity risks given the Group's approach to paying the external and subsidiary dividends. These risks are also relevant for the longer time periods.</p> <p><b>Resilience</b></p> <p>The Group generates relatively steady cash profits on new business and existing funds under management which we would expect to increase each year as funds in gestation 'mature'. If severe risks materialised over the year and resulted in significant costs, the Group would have options to deal with the financial implications. Whilst other options would be explored first, curtailing investment or reducing dividends would be obvious ways to protect the financial strength of the business.</p> <p>Operational resilience and business continuity are also important and risks which might cause severe business disruption are carefully managed.</p> <p>There are not considered to be any material uncertainties over the ability of the Group to survive over the one-year time horizon.</p>	<p><b>Risks</b></p> <p>Investor sentiment, market impacts, changes to regulation following Brexit and tax changes following the UK Government's relief strategy for COVID-19 continue to provide uncertainty.</p> <p>Aside from COVID-19 and Brexit, risk relating to changes to advice regulation would likely impact the business in the next five years, or beyond.</p> <p>The importance of technology in the client proposition is only likely to become more important and risks may materialise from non-traditional competitors seeking to disrupt the UK financial advice market.</p> <p>Risks which have a more gradual effect, such as talent retention and acquisition, are also relatively more important over a longer time horizon.</p> <p><b>Resilience</b></p> <p>Counteracting the medium-term risks, there is more time to respond and take actions to manage the Group's prospects. As already referenced stress and scenario testing (such as the COVID-19 scenario) takes place which provides comfort over the Group's ability to weather storms over a five-year time horizon and adapt. The Group's strategy is designed to navigate the threats and keep our proposition current for existing and potential clients. As the largest wealth manager in the UK the Group is well resourced to effectively respond to regulatory change and deal with increased regulatory complexity.</p>	<p><b>Risks</b></p> <p>Most of the shorter-term risks will remain relevant, however, over the longer-term, client expectations around digital services are likely to become more important. The impact of artificial intelligence and machine learning on both the investment management and advice spaces will become more prevalent.</p> <p>Risks from climate change are starting to have an impact on investor sentiment and drive political change and this is only likely to increase. Beyond 2024 climate change is likely to be a far more significant factor for many of our clients.</p> <p><b>Resilience</b></p> <p>Whilst the importance of technology in the advice space will grow, we believe that overall our target market will continue to value human interaction in discussing sensitive financial matters. We recognise however that the advice proposition will develop, and our advisers will need to be technology-enabled. With increased use of integrated technology, we will be able to automate processes and allow our advisers to focus on the high-value advice and service aspects.</p> <p>We have been developing our responsible investing proposition for some years and welcome the focus in this area as the right thing to do and as an opportunity to maximise client benefit through our active Investment Management Approach.</p>

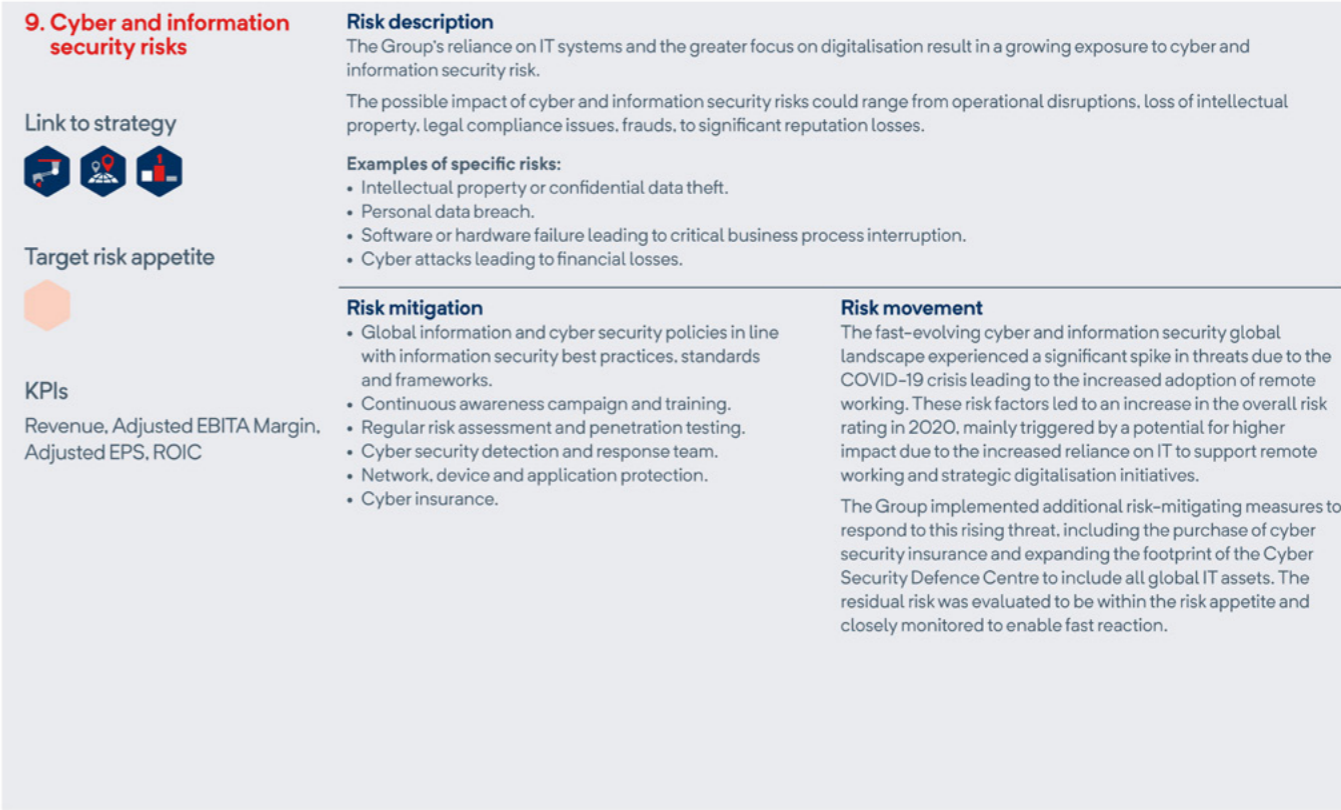
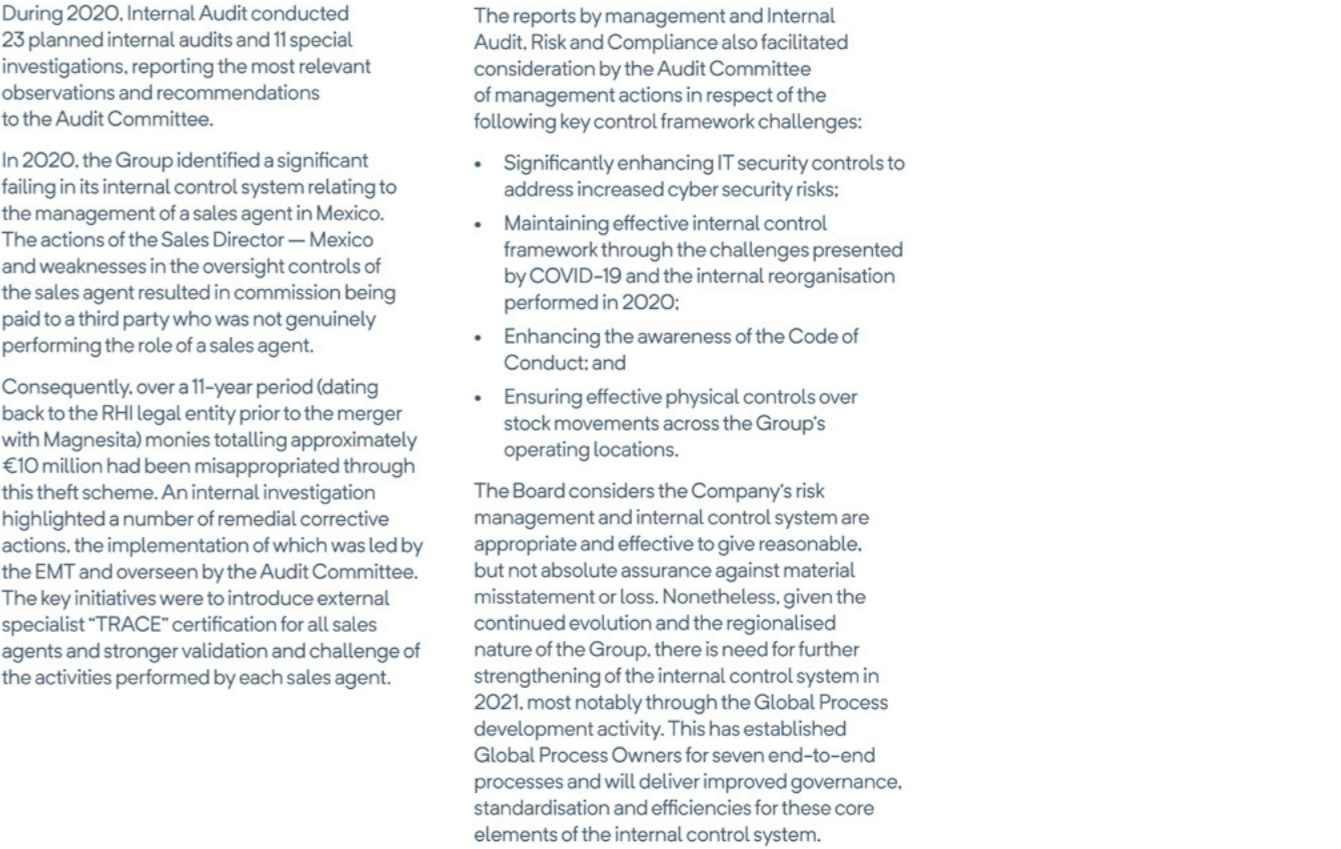
**Conclusion**  
In accordance with the UK Corporate Governance Code (Provision 31), the Directors have assessed the Group's current financial position and prospects over the next five-year period and have a reasonable expectation that the Group will be able to continue in operation and meet its liabilities as they fall due. The Directors believe that the Group's risk planning, management processes and culture allow for a robust and effective risk management environment.

In addition to the assessment of longer-term viability and resilience set out above, the Board has assessed the Group's going concern status. Further information is provided in the Directors' Report on page 140.

**Figure 2.9**  
Grafton: Programme to perform fraud risk assessment; fraud as a constituent of a principal risk (2020 ARA, p65)



**Figure 2.10**  
RHI Magnesita: Increased IT security controls and fraud not prevented by internal controls (2020 ARA, pp51 and 58)



**Figure 2.11**  
**Derwent London:** ‘Risk of business interruption’ as a principal risk split into three sub-risks, two of which relate to cyber: ‘cyber attack on our IT systems’ and ‘cyber attack on our buildings’ (2020 ARA, p94)

Risk	Our key controls
<div>6. Risk of business interruption</div> <div>a. Cyber attack on our IT systems</div> <p>The Group is subject to a cyber attack that results in it being unable to use its IT systems and/or losing data. This could lead to an increase in costs whilst a significant diversion of management time would have a wider impact. Considerable time has been spent assessing cyber risk and strengthening our controls and procedures.</p> <p><b>Movement during 2020:</b> Increased</p> <p>During 2020, there has been an increase in cyber attacks being perpetrated as cyber criminals seek to exploit Covid-19. In response, we identified the key IT risks arising from home working and implemented additional controls.</p> <p><b>Executive responsibility:</b> Damian Wisniewski</p>	
<div>b. Cyber attack on our buildings</div> <p>The Group is subject to a cyber attack that results in data breaches or significant disruption to IT-enabled tenant services. Buildings are becoming ‘intelligent’, with an increase in internet enabled devices broadening the cyber security threat landscape.</p> <p><b>Movement during 2020:</b> Unchanged</p> <p>The potential impact of a cyber attack on our buildings has reduced due to the winding down of services and overall low occupancy caused by Covid-19. Conversely, the potential risk of this occurring has increased due to low occupancy levels which could provide an opportunity for attack. During the lockdown, 24/7 security was provided by outsourced providers.</p> <p><b>Executive responsibility:</b> David Silverman</p>	
<div>c. Significant business interruption (for example, pandemic, terrorism-related event or other business interruption) (previously, ‘Terrorism-related or other business interruption’)</div> <p>The risk that a pandemic, terrorism-related event or other business interruption causes significant business interruption to the Group and/or its occupiers or supply chain. This could result in issues such as inability to access or operate our properties, tenant failures or reduced rental income, share price volatility, loss of key suppliers, etc.</p> <p><b>Movement during 2020:</b> Increased</p> <p>Covid-19 has caused significant business interruption for some of our occupiers, particularly retail, travel, restaurants or other leisure services. During 2020, there has been limited business interruption for Derwent London; however, the lockdown has caused a delay to our development activities and reduction in cash flow due to deferment, concessions or non-payment of rent.</p> <p><b>Executive responsibility:</b> All Executive Directors</p>	

**Figure 2.12**  
**Mondi:** Insight on activities undertaken to oversee cyber as well as the frequency of the assessment (2020 ARA, p120)

<p><b>Information technology risk</b></p> <p>The committee undertakes, on a half-yearly basis, a detailed review of information technology risk and mitigation actions. The Group’s IT risk management framework has been explained to the committee, with comfort obtained that it is holistic and robust, having been audited by independent third parties.</p> <p>While these reviews cover all relevant aspects of IT risk, including security, compliance and availability, the focus is increasingly on cyber security, with the top five IT risks being in this area. Cyber security drives the principal mitigation activities, particularly in the areas of network design and security architecture. Lessons learnt from attempted security breaches and cyber security training for employees were key areas of focus for the committee during the year. The launch of a new cyber security awareness campaign was particularly successful, teaching employees how to better protect themselves. ISO 27001 certification was also obtained. The committee was encouraged by the level of focus being given to cyber security across the Group and the emphasis being placed on employee awareness, education and testing was welcomed.</p>	<p>The significant increase in the number of employees working from home due to COVID-19 was also a challenge this year. Work was undertaken at very short notice to ensure stable and effective remote access to the Mondi network and that reliable methods of communication and the ability to hold virtual meetings were readily available. At the same time, security was a priority. The key actions taken were monitored by the committee. These included the development of a taskforce to monitor system performance, guidelines to help employees work from home effectively and the expansion of the virtual meeting functionality, as well as the continuation of cyber security training. The committee was comfortable that the response had been appropriate, with systems remaining stable and secure throughout the pandemic.</p> <p>Overall the committee concluded that the Group’s IT risk management was effective and that management ensured that it was subject to continuous monitoring and improvement (see pages 84-85 for more information).</p>
---	--

## Authors



**Mala Shah-Coulon**

Associate Partner, Head  
of Corporate Governance  
mshahcoulon@uk.ey.com  
+44 (0)20 7951 0355



**Maria Kępa**

Director, Assurance  
mkepa@uk.ey.com  
+44 (0)7795 645183

We thank Beatriz Diego, Vicky Johnson, Samantha Chew, Bidushee Biswas, Marete Pretorius, Eduardo Gispert, Gavin Cartwright, Bob Ward, Tom Garside, Mary Buxton, Neil Mathur, Amarjit Singh, Emma Price, Jonathan Middup, Daniel Feather and Peter Scoffham for all their help in producing this report.

## EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organisation, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via [ey.com/privacy](https://ey.com/privacy). EY member firms do not practice law where prohibited by local laws. For more information about our organisation, please visit [ey.com](https://ey.com).

© 2021 EYGM Limited.  
All Rights Reserved.

EYSCORE 006129-21-UK  
Artwork by JDJ Creative Ltd.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

[ey.com](https://ey.com)