




2024 UK Corporate Governance Code

Addressing the new risk management and internal control requirements, including Provision 29

August 2024

Contents

1	Introduction	1
2	Changes to governance and processes	5
2.1.	Basic tenets	5
2.2.	Material controls	5
2.2.1.	Defining material controls	5
2.2.2.	Types of material controls	7
2.2.3.	Number of material controls	8
2.3.	Effectiveness of material controls	10
2.3.1.	Defining effectiveness	10
2.3.2.	Agreeing the target level of confidence over the effectiveness of material controls	10
2.3.3.	Explain rather than comply	12
2.4.	Monitoring and review of the framework	12
2.4.1.	Board-level monitoring	12
2.4.2.	Board-level review	13
2.5.	Role of the board and its sub-committees	14



3 Enhancements to reporting	16
3.1. Overview	16
3.2. Re-ordering the flow	17
3.3. Risk management and internal control framework	18
3.3.1. Risk management process	18
3.3.2. Internal control framework	19
3.4. Principal risk disclosure	20
3.4.1. Mitigating actions	20
3.4.2. Additional risk attributes	20
3.5. Reporting on governance activities	21
3.5.1. Aspects of current practice that will need to evolve	21
3.5.2. Good practice governance reporting	22
3.6. The declaration	24
3.6.1. Reporting ineffectiveness	24
3.6.2. Providing explanations	24
4 Next steps	25
Appendix: Illustrative examples	27

Section 1

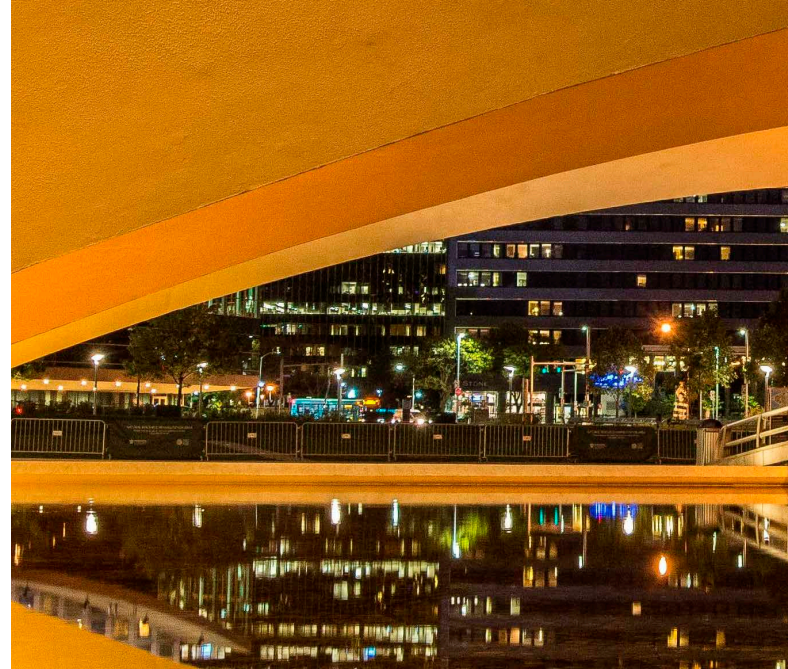
Introduction

Having had numerous conversations with boards and senior management on risk management and internal controls since the Financial Reporting Council (FRC) issued the 2024 UK Corporate Governance Code (the Code) in January 2024, we have often found ourselves going back to the history of how we got to where we are. This is partly due to nearly six years elapsing since these changes were first mooted, but largely, it is because of the need to understand the spirit of the changes, too.

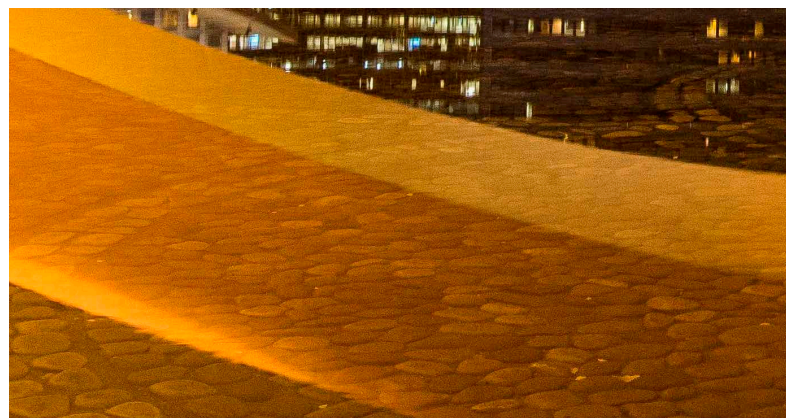
Following the collapses of Carillion and BHS, the UK government commissioned independent reviews relating to the quality and effectiveness of audit (the Brydon Review), and the Financial Reporting Council (the Kingman Review).

In relation to internal controls:

- ▶ The Kingman Review of 2018 recommended that the then UK government seriously considers the case for a strengthened framework around internal controls in the UK and learn any relevant lessons from the operation of the Sarbanes-Oxley (US SOX) regime in the US.
- ▶ The Brydon Review of 2019 furthered this by recommending that the UK government gives serious consideration to mandating a UK Internal Controls Statement consisting of a signed attestation by the chief executive officer (CEO) and the chief financial officer (CFO) to the board that an evaluation of the effectiveness of the company's internal controls over financial reporting has been completed and whether or not they were effective.



The UK government consulted on these recommendations in 2021 as part of 'Restoring trust in audit and corporate governance'. Its preferred option was an explicit statement from the directors on the outcomes from their annual review of the effectiveness of the company's internal controls over financial reporting, supported by disclosures on the benchmark system used and an explanation of how directors had assured themselves that it was appropriate to make the statement, but not mandating external assurance. However, in parallel, the regulator would have powers to investigate the accuracy and completeness of the directors' internal control disclosures and, if necessary, order amendments or recommend an external audit of the internal controls. There would also be powers to sanction directors where they failed to establish and maintain an adequate internal control structure and procedures for financial reporting.





In 2022, when publishing the consultation's outcome, the UK government expressed concerns that putting a directors' statement on a legislative footing might, in practice, lead companies to default to external assurance from their auditors as the safest way of avoiding challenge. This, in turn, could affect the attractiveness of the UK's public markets as a place to list. As such, it decided to take a Code-based approach instead and invited the FRC to consult on strengthening the internal control provisions in the Code and to issue guidance on how boards should approach the preparation of the statement. It also noted that the principles-based approach would be particularly effective if investors in their stewardship role applied pressure on boards where internal controls seemed weak or where directors' statements were 'boilerplate' or inadequate. The UK government did, however, at that time intend to introduce secondary legislation on reporting, such as

the 'audit and assurance policy', to supplement the Code's requirements and also establish a stronger regulator – the Audit, Reporting and Governance Authority (ARGA) – to succeed the FRC.

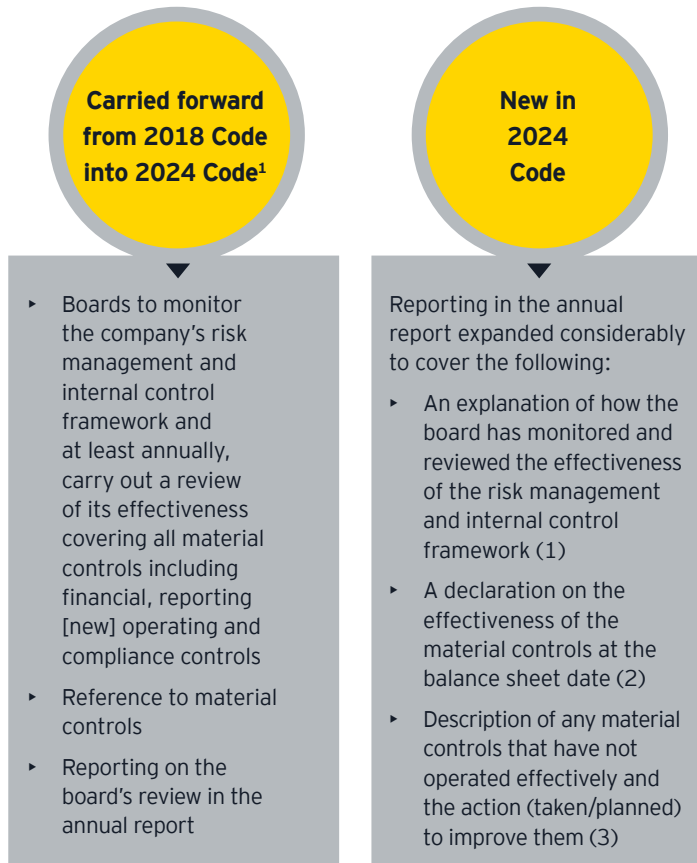
Before the FRC had the opportunity to publish the response to its consultation on the Code, the UK government had withdrawn the aforementioned secondary legislation. It had also become clear that the primary legislation to introduce ARGA would be delayed.

Against this backdrop, in January 2024, the FRC published the updated 2024 UK Corporate Governance Code and, soon after, provided supporting guidance. The main change, effective for periods beginning on or after 1 January 2026, six years after the Brydon review, concerns strengthened risk management and internal control requirements reflected in the updated Provision 29.

Provision 29 of the 2018 Code was already quite broad. In crafting the final wording of the provision, the FRC took on board views expressed by a group of audit committee chairs as part of the UK government's consultation. Those audit committee chairs *"agreed that there was a need for the reporting about internal controls to be improved to help build investor confidence and sharpen directors' accountability. However, they questioned the implication that there was a general need to strengthen the systems themselves in large UK companies."*



Principle O now references the need for boards not only to establish, but also maintain the risk management and internal control framework. However, the main thrust of the changes is to upgrade disclosures previously recommended by the guidance into the Code's requirements:



To emphasise the importance of clear reporting, Richard Moriarty, the CEO of the FRC, has often referred to Provision 29 as the 'transparency provision'. In fact, the FRC has stated on several occasions that its objective is to bring reporting of all FTSE companies in this area to the standard already demonstrated by the best reporters.

Nonetheless, based on our conversations, the fact that directors have to make an explicit declaration on the effectiveness of material controls is causing many companies and their boards to consider whether they need to do more than enhance their reporting. Some are also using this as an opportunity to explore integrated assurance and assurance mapping and re-enforce consideration of emerging risk and risk scenarios. This may help enhance understanding of organisational resilience.

Reporting should offer transparency on the risk and internal control framework that is operating with the company. In some cases, the current reporting may convey the quality of the controls system; in others, the improved reporting requirement we hope will raise standards.

FRC Q&A

Notes

Under the 2018 Code:

1. Directors were *encouraged through guidance* to set out what the review of the system of risk management and internal controls entailed; now, they will be required by the Code to do so and additionally describe the monitoring that was undertaken.
2. Directors had to report on their review of the effectiveness of risk management and internal controls systems; now, they will have to provide an outcome based on this: a declaration on the effectiveness of material controls as at the balance sheet date.
3. Directors were *encouraged through guidance* to set out actions undertaken to address failings or weaknesses; now, they will be required to describe those material controls that were not operating effectively and the actions (taken or proposed) to improve them.

1. 2018 Code Provision 29: The board should monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness and report on that review in the annual report. The monitoring and review should cover all material controls, including financial, operational and compliance controls.

As is the case with other aspects of Code-related disclosures, there is no specific oversight for this type of reporting. The King's Speech of July 2024 noted the UK government's intention to publish a Draft Audit Reform and Corporate Governance Bill, which, among other measures, would establish ARGAs with appropriate powers. Whilst it will be interesting to see whether the timing of this coincides with when companies make their first declarations, until there is certainty on its establishment, the scope of its powers and how they would be exercised, there are no formal enforcement mechanisms in the form of sanctions or penalties. However, companies need to be cognisant of the UK Listing Rule (UKLR) requirements too – in particular, Listing Principle 1 in [UKLR 2.2.1R](#): "A listed company must take reasonable steps to establish and maintain adequate procedures, systems and controls to enable it to comply with its obligations." Related guidance in [UKLR 2.2.2G](#) explains that this principle is intended to ensure that listed companies:

“have adequate procedures, systems and controls to enable them to comply with their obligations under the listing rules, disclosure requirements, transparency rules and corporate governance rules”.

The structure of this publication

It is important to consider Provision 29 from two perspectives:

- ▶ The changes that may be required to underlying processes – Section 2 of this publication.
- ▶ The enhancements needed to reporting – Section 3 of this publication.

It is also important to use common language. For this reason, throughout this document, when referring to:

- ▶ Elements of a risk management and internal controls framework, we use terminology from the **COSO framework** developed by the Committee of Sponsoring Organizations of the Treadway Commission.² This is not because we are advocating its application but rather because the terms it uses are well-understood.
- ▶ The first, second or third line to describe where certain activities are being undertaken, we refer to the **Three Lines Model**, developed by the Institute of Internal Auditors to help organisations implement risk management.³
- ▶ Categorisations of controls, we use:
 - ▶ Entity-level controls – that pervasively impact an entity’s environment and operations. They include rules, standards of conduct, policies and procedures. These controls are the foundation that allows all other controls, processes and programmes to function effectively.
 - ▶ Transaction-level controls – embedded within individual processes that can be manual, dependent on information technology (IT), or automated.
 - ▶ General IT controls – that provide a set of directives for controlling how IT solutions, systems and resources are used and managed.

The observations and recommendations that follow are based, amongst others, on our conversations with companies working towards compliance and on reading the risk management and internal control narratives across annual reports. We also draw on statements made by the FRC, including in its guidance to the Code. As we provided detailed references to the guidance in our **summary**, we have not always repeated them in this analysis.

2. *Internal Control – Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission, 2013.

3. *The IIA’s Three Lines Model: An update of the Three Lines of Defense*, The Institute of Internal Auditors, 2020.

Section 2

Changes to governance and processes



2.1. Basic tenets

- ▶ The Code must be sufficiently flexible to be applied by both the largest and most complex FTSE 100 entities as well as by smaller FTSE companies. This lends itself to a proportionate, flexible and customisable rather than prescriptive approach.
- ▶ The FRC has not defined ‘material controls’ and has unequivocally stated that this is the responsibility of the board. This necessitates a top-down, board-led approach. However, there should be no misconception that material controls alone will be sufficient to provide reasonable assurance on the achievement of an entity’s objectives. This top-down approach to controls should be supported by a robust bottom-up foundation.
- ▶ The supporting FRC guidance is high-level, not part of the Code and not mandatory. It is designed to stimulate thinking and aid boards in their actions and decisions when applying the Code.
- ▶ For the approach to be both effective and efficient, it is essential not to re-invent existing processes or start from scratch. The starting point is first to analyse how extant risk management and internal control requirements, e.g., in the 2018 Code and the Disclosure Guidance and Transparency Rules (DTR), are being met and then to determine how these can be leveraged.⁴ Equally, companies

should capitalise on existing programmes. These may include ongoing initiatives to enhance internal controls over financial reporting, conducting risk assessments to comply with the European Union’s Corporate Sustainability Reporting Directive or implementing measures in anticipation of the failure to prevent fraud offences becoming effective.

There is no expectation that companies with a robust risk management and internal control framework already in place are required to change how they operate. For example, companies that already have a process to comply with US SOX can designate that process as a material control.

2.2. Material controls

Material controls are not a new concept – the 2018 Code already used this terminology. However, the 2024 Code now also references reporting controls in addition to the previous financial, operational, and compliance controls. Whilst material controls should cover these four categories, they are not necessarily limited to these.

2.2.1. Defining material controls

Whilst not new, the fact that the boards now have to provide a specific declaration of their effectiveness is causing companies and boards to closely consider what these are. The board will need to maintain a defined but dynamic list that it will monitor.

4. DTR 7.1.3 R An issuer must ensure that, as a minimum, the relevant body must:

1. Monitor the financial reporting process and submit recommendations or proposals to ensure its integrity
2. Monitor the effectiveness of the issuer’s internal quality control and risk management systems and, where applicable, its internal audit regarding the financial reporting of the issuer without breaching its independence



Whilst there is no definition of a material control, the following considerations may help boards in their determination:

- ▶ The potential impact of how a deficiency in a control could impact the company, its shareholders and other stakeholders
- ▶ The extent to which controls help maintain principal risks within the board's defined risk appetite

We advocate for considering material controls through the following two lenses:

- ▶ **Addressing the risk of material errors in both financial and non-financial reporting.**

Principle M of the Code sets out that the board should satisfy itself on the integrity of financial and narrative statements. DTR 7.1.3R also has similar requirements in relation to financial reporting, as detailed in footnote 4. Material information that stakeholders, and especially investors, rely on for decision-making, as well as price-sensitive information, needs to be free from material errors. Material controls over the reliability of such reported information can be referred to in the aggregate as material controls over disclosures.

Other practical considerations

Use this as an opportunity to review the company's external reporting to identify whether certain disclosures that have accumulated over time but lost their importance, have been superseded, and are effectively covered by new requirements, can be eliminated. Those disclosures that remain relevant should be prioritised by reference to criteria that determine their significance.

- ▶ **Mitigating principal risks that could affect the long-term sustainability of the business.**

Not every principal risk needs to be managed or mitigated to the same extent. Boards may decide that, for example, controls in respect of principal risks not included within viability statement scenarios do not meet the definition of a material control or that principal risks with a high risk appetite require fewer material controls than those where the risk appetite is low.

Furthermore, companies should not become preoccupied with categorising material controls as operational, compliance, or otherwise. The objective of the material control matters, not its categorisation. For instance, in a mining company, several material controls might be in place to prevent a tailings dam collapse, ranging from financial controls such as capital expenditure approval to operational and compliance controls like internal policies and independent safety checks.

Other practical considerations

Use this as an opportunity to review how principal risks are worded and how underlying risks are grouped into principal risks.

FRC Guidance (para 272): material controls could include, but are not limited to controls over:

- ▶ External reporting that is price sensitive or that could lead investors to make investment decisions, whether in the company or otherwise



Financial reporting

Non-financial reporting

- ▶ Risks that could threaten the company's business model, future performance, solvency or liquidity and reputation
- ▶ Fraud, including override of controls
- ▶ IT risks including cybersecurity, data protection and new technologies



Principal risks (in viability scenarios)

Principal risks (other)

Other risks

Code Principle M:

The board should (...) satisfy itself on the integrity of financial and narrative statements.

FRC Guidance (para 250)

Controls implemented should be appropriate to maintain these risks within the defined risk appetite.

2.2.2. Types of material controls

Controls that operate lower down in the organisation, often within the first line, tend to have a narrow focus. Whilst the board has full discretion to define its material controls, we expect that directors will prefer to assess the operational effectiveness of a smaller number of more pervasive controls performed at higher levels in the organisation.

In the first instance, we expect that boards may consider existing aspects of the company's risk management and internal control framework and:

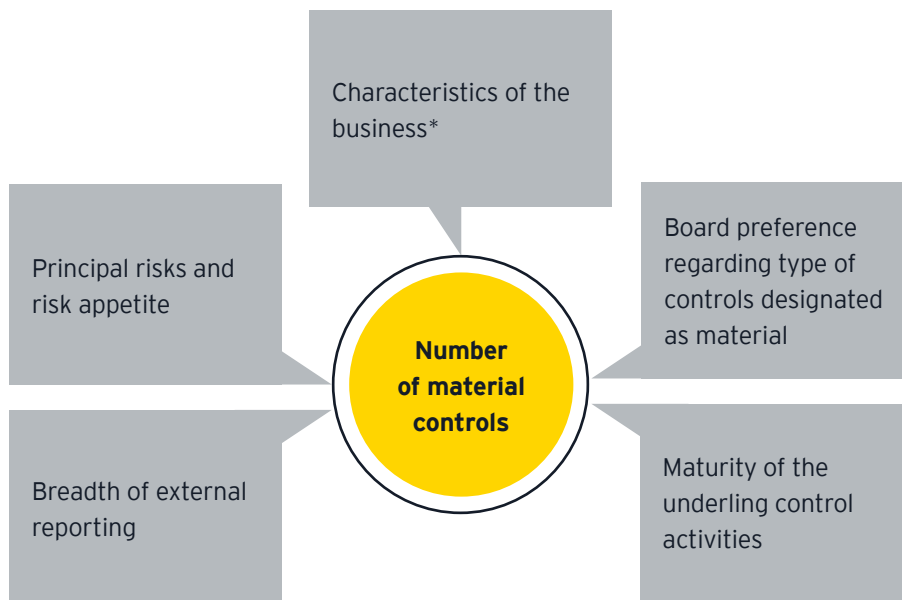
- ▶ Choose to focus on entity-level controls that form part of the overall control environment, such as code of conduct and whistleblowing arrangements
- ▶ Designate parts of the internal control framework, such as any risk monitoring programme within the second line, to be a material control
- ▶ Request reporting on how controls such as segregation of duties or delegation of authority have been adhered to overall

- ▶ Want certain transaction-level controls to be aggregated into groupings of preventing, detecting and compensating controls to create a sufficiently elevated material control
- ▶ Determine whether certain processes that are being performed but not presently classified as material controls can be designated as such. For example, the board of a company subject to US SOX requirements may designate the process that results in the attestation signed by the CEO and CFO as a material control.

In some instances, however, introducing completely new material controls may be more efficient. For example, some companies are establishing additional management committees tasked with overseeing specific areas of risk and related controls. As long as these are executive committees, this approach appears to be acceptable. However, and in line with COSO, we do not consider it appropriate to classify activities undertaken by the board or its committees as a material control. Of course, such independent oversight constitutes a vital part of the overall internal control framework but is not a material control in its own right.

2.2.3. Number of material controls

There is no set benchmark for the number of controls a board should consider material. This will depend on several factors, many of which are company-specific, as shown below:



*e.g., decentralisation, geographic footprint and regulatory burden

The number will also depend on the board's preference. One board may prefer to receive reporting on more controls that are slightly less aggregated; another may prefer fewer, higher-level controls, e.g., the aforementioned executive committees. This preference may differ between material controls over disclosures and those related to principal risks.





Material controls are, by their nature, operating at a higher level within the organisation. They often rely on underlying business and IT controls to support them. Effective material controls require effective underlying controls.

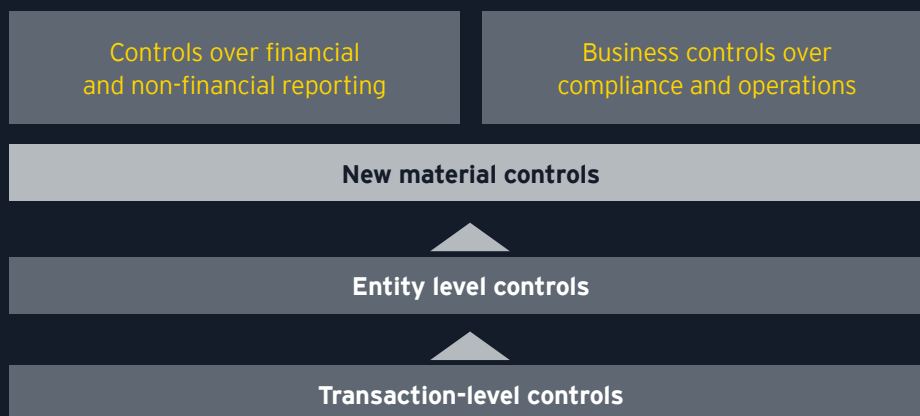
For example, a material control could involve a specialist compliance team that monitors exceptions to a suite of policies and procedures, ensuring they are followed up and resolved on a timely basis. This control depends on several lower-level controls, such as:

- ▶ **An exception reporting process being in place**
- ▶ **Policies being rolled out**
- ▶ **Employees receiving adequate training on those policies and procedures**
- ▶ **IT systems configured to prevent unauthorised changes to the exception reporting workflow**

We supported many companies in strengthening internal controls over financial reporting, particularly when the exact outcomes of revising the Code were uncertain. We deployed our 'minimum controls tool' to help companies mitigate the most risks with the fewest controls.

Building on this success, we have expanded our minimum controls tool to address non-financial reporting as well as operational and compliance risks.

Our methodology ensures that the company implements an efficient and agile internal control framework that can be maintained and that will support the board in making its declaration on the effectiveness of material controls.



For more information on this approach, please contact:



Daniel Feather
Partner, Ernst & Young LLP
Email: dfeather@uk.ey.com

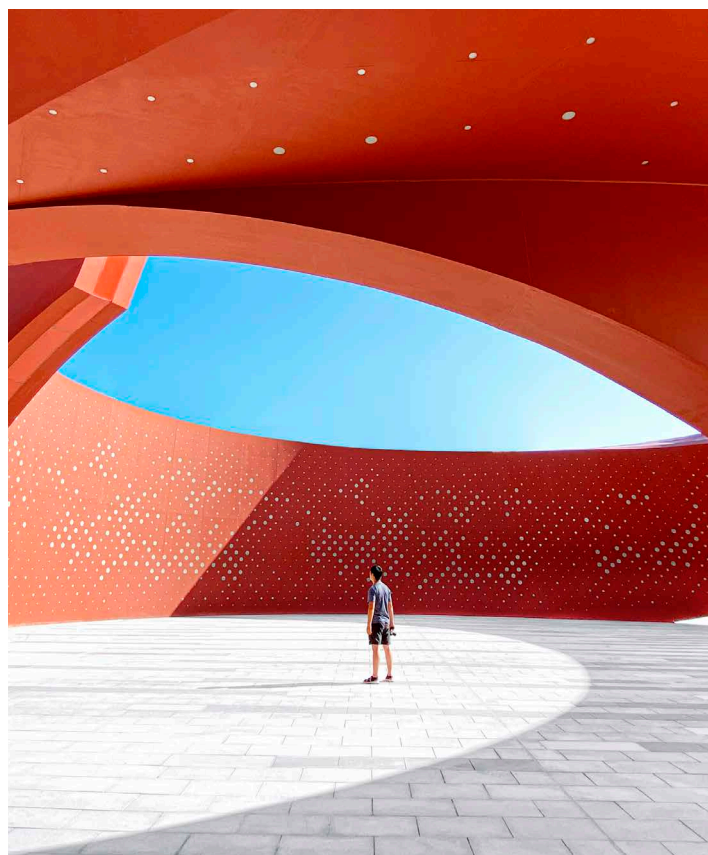
2.3. Effectiveness of material controls

Agreeing on a list of material controls is the first step; the next step is to define the criteria for their effective operation. Boards will then need to determine what evidence they need to conclude whether the criteria have been met.

2.3.1. Defining effectiveness

Defining the effectiveness of material controls will be less straightforward and more judgemental than defining the operational effectiveness of transaction-level controls where the decision is more binary. Documentation of material controls will help with this step.

Whilst even in established control regimes such as COSO, there is no single definition of what documentation should exist to support the existence of effective controls, COSO does describe the nature and extent of documentation that should be retained, depending on the nature of the risk being managed. As such, COSO may help determine the documentation required to support the board's assessment. COSO may also be a reference point for any assurance provider asked to evaluate one or more material controls.



It is only with clearly defined control requirements, such as the extent of processes and policies and frequency of operation, that the board will be able to determine if the material controls are working effectively or not. When an entity does not have a formalised and documented risk management and internal control framework, whilst not required, at the very least, directors should consider whether material controls may require formalised documentation.

By defining effectiveness, directors can establish which material controls have not operated effectively and what requires disclosure under Provision 29. We also recommend that directors clarify the criteria for an internal escalation process for weaknesses in the operation of material controls where the internal control system only narrowly achieves the desired outcome. Such weaknesses can be indicators that the control could fail at year-end. In its guidance, the FRC refers to these as 'near misses'.

2.3.2. Agreeing the target level of confidence over the effectiveness of material controls

The FRC's guidance states that the board should form its own view on the effectiveness of material controls. This view should be based on two elements: firstly, the board's monitoring and review of the risk management and internal control framework, and secondly, robust, appropriately documented evidence obtained by the board.

The FRC's guidance does not specify what such documentation should cover, but it does emphasise that there is no requirement or expectation that companies obtain external advice or assurance on the effectiveness of the material controls. There is also no explicit requirement for internal assurance. Consequently, we use the term 'target level of confidence' rather than 'assurance' to reflect this flexibility.

When establishing if a control is operating effectively at year-end, the board should also consider whether its design remains appropriate in light of any changes and events that may have arisen during the year.

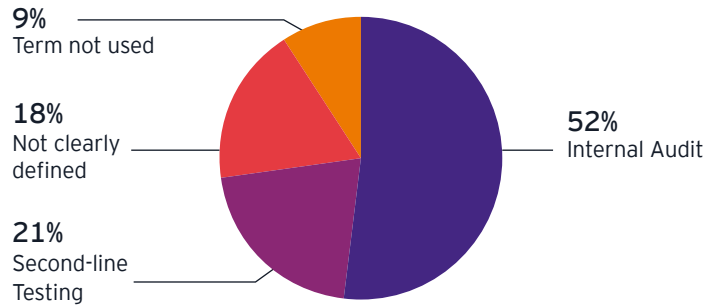
Therefore, the board must make decisions about:

- ▶ The target level of confidence it will require (whether internal or external); this does not need to be uniform across all controls.
- ▶ The precision of documentation and evidence required to reach its conclusions.
- ▶ The frequency of reporting underpinning its monitoring activities.

Companies that had started developing an audit and assurance policy before the related secondary legislation was withdrawn are finding it a useful starting point for determining their target level of confidence. Similarly, existing assurance maps are proving helpful in conducting gap analyses between the actual and target levels of confidence.

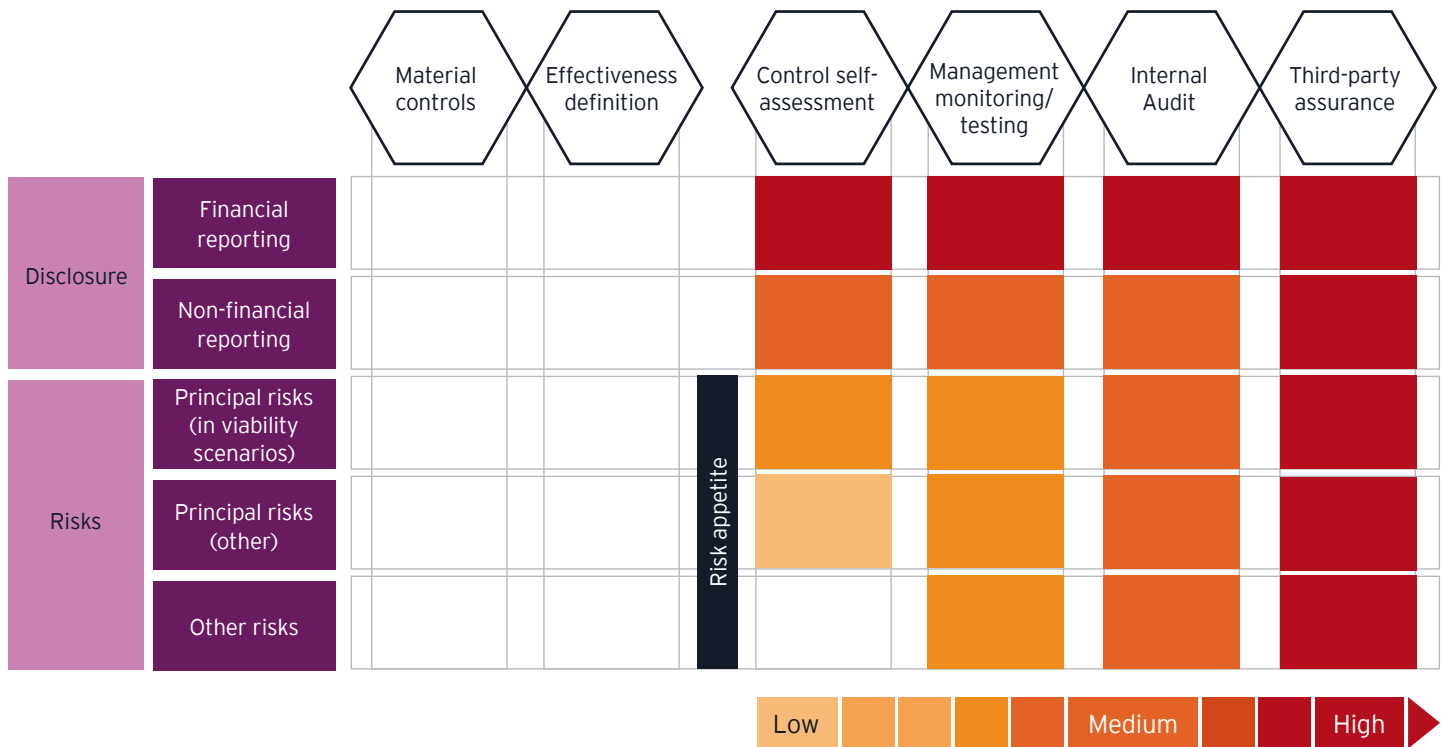
Wording used in annual reports indicates that the attribution of the term 'assurance' to activities undertaken internally by organisations, varies. More than half of companies apply it only in the context of internal audit. Approximately 20% also refer to assurance provided by second-line testing and, in rare instances, even first-line self-certifications. A further 20% mention assurance activities without clearly defining the assurance provider.

Use of the term assurance



These reporting observations may indicate that companies need to develop and communicate a common understanding of the level of confidence derived from internal activities undertaken by the first and second line. It also requires being clear on the different types of activities undertaken by internal audit and the level of assurance that these provide.

Agreeing the level of confidence required by the board



2.3.3. Explain rather than comply

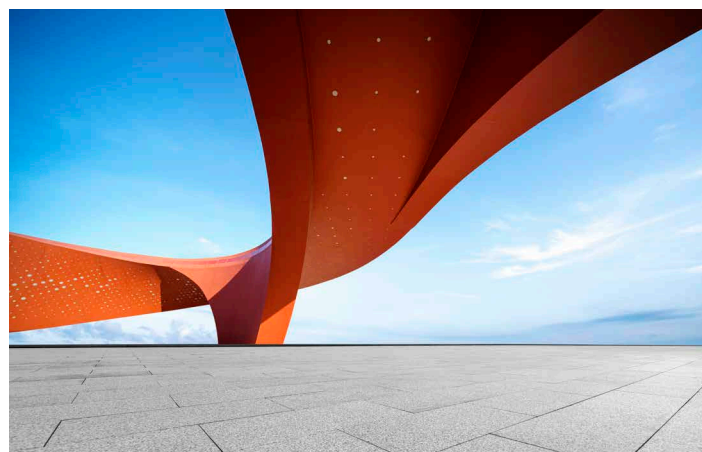
As the Code operates on a comply-or-explain basis, in some cases, the board may caveat that the declaration does not cover certain material controls or material controls over certain areas and explain why. For example, a board may conclude that it is not efficient to assess the effectiveness of certain material IT general controls during a major systems implementation or migration. Or it may conclude that certain areas of internal control are insufficiently mature to be assessed. However, if these relate to disclosures, the board should remain cognisant of obligations arising from the Listing Principles. The FCA's Primary Market Technical Note 801.1 of December 2020 succinctly explains these obligations.⁵ Specifically, it highlights that listed companies need to have adequate systems for collecting material environmental, social, and governance data.

Declaring that a material control had not operated effectively as at the year-end is not 'non-compliance'. When identifying ineffective material controls, boards will need not only to consider the potential reputational impacts but also whether the company is meeting its obligations under these Listing Principles.

Listing Principle 1 in UKLR 2.2.1R: A listed company must take reasonable steps to establish and maintain adequate procedures, systems and controls to enable it to comply with its obligations.

UKLR 2.2.4 G: Timely and accurate disclosure of information to the market is a key obligation of listed companies. For the purposes of Listing Principle 1, a listed company should have adequate procedures, systems and controls to be able to:

1. Ensure that it can properly identify information which requires disclosure under the listing rules, disclosure requirements, transparency rules or corporate governance rules in a timely manner
2. Ensure that any information identified under (1) is properly considered by the directors and that such a consideration encompasses whether the information should be disclosed.



2.4. Monitoring and review of the framework

The FRC guidance explains that the risk management and internal control framework encompasses policies, culture, organisation, behaviours, processes, systems and other aspects. Whilst the board could use a recognised framework or standard to design and maintain a company's framework, it does not have to do so. However, the board has to monitor and review the framework. The FRC guidance considers company-level monitoring, board-level monitoring and board-level review of the risk management and internal control framework to be three separate concepts.

2.4.1. Board-level monitoring

Under the COSO framework, monitoring activity is conducted by management to assess whether controls within each of the five components of internal control are operating as intended. According to the FRC guidance, monitoring does not relate only to controls but encompasses the monitoring of risks as well. Furthermore, the board cannot rely solely on the embedded monitoring processes within the company but should conduct its own monitoring, which includes oversight of the procedures established at the company level.

The board's monitoring will likely encompass regular reporting and other communication with management, internal audit, external audit, and individuals from various specialist functions or business units across the company.

5. As this was issued in 2020, it contains references to the previous Listing Rules, rather than the new UK Listing Rules effective from 29 July 2024. However, both the Listing Principle and the related guidance remain unchanged.

When determining their approach to the monitoring of the risk management and internal control framework, boards may find **recent observations** from the FCA in relation to its review of larger insurance firms' approaches to outcomes monitoring under the Consumer Duty, of interest.

... many firms need to make improvements in their monitoring to enable them to determine whether they are delivering good outcomes for retail customers, as required by the Duty.

For example:

- ▶ Some approaches were overly focused on processes being completed rather than on outcomes delivered. Some board or committee reporting contained limited insight into actual customer outcomes. This was often because of:
 - ▶ Metrics/data not being comprehensive enough

- ▶ Data which lacked analysis and explanation
- ▶ Thresholds/standards in place which did not appear to be appropriately set and/or communicated.
- ▶ Few firms were able to provide clear evidence of where the monitoring of outcomes had directly led to proactive action being taken to improve these outcomes, where necessary.

While inadequate monitoring itself would not necessarily result in poor customer outcomes, monitoring is essential for firms to identify and remediate them.

Source: FCA, Multi-firm review, June 2024

The board will need to specify the formality, scope and frequency of such regular communications, with a special focus on previously reported issues and weaknesses in the operation of material controls and actions being taken to address them. It may also wish to compile a list of data points or event types (e.g., regulatory breaches or fines) that would trigger the need for ad hoc communication.

Monitoring should not be done for the sake of it, rather to ensure that timely actions are taken where needed. It should lead to timely remediation activities and the redesign of material controls, if required. Any list of material controls agreed on at the beginning of the year should be updated to reflect matters such as changes in the risk profile, acquisition activity, system implementations, etc.

Other practical considerations

The Economic Crime and Corporate Transparency Act 2023 introduced a new corporate 'failure to prevent' fraud offence, making a company criminally liable if it fails to prevent a fraudulent act perpetrated by one of its associated persons. If not already part of business-as-usual (BAU) operations, companies should begin conducting fraud risk assessments to identify higher-risk areas and control gaps in their fraud framework. Regular and effective monitoring will reduce the likelihood that a company will fall foul of the offence. Documenting the activity and results will help the company in any future defence.

2.4.2. Board-level review

Both monitoring and review serve to identify and evaluate areas for improvement in the design, implementation and operation of the entire risk management and internal control framework. The distinction we make is that:

- ▶ The former is an ongoing or regularly scheduled activity that does not require an effective conclusion.
- ▶ The latter is conducted at a specific time, such as at or close to the balance sheet date, and leads to a conclusion on the effectiveness of material controls. According to the FRC guidance, the review should also evaluate the effectiveness of the monitoring process.

It is for the board to decide how it will conduct the review and leverage its monitoring activities. As noted in the introduction, the requirement for the board to review the effectiveness of risk management and internal controls, including all material controls, at least annually, has not changed from the 2018 Code. What has changed is the need to provide the declaration of effectiveness of individual material controls. Boards will, therefore, need to consider how their existing review process and the reporting they receive need to be adapted to give them visibility into the operation and effectiveness of material controls instead of just into the overall framework.

2.5. Role of the board and its sub-committees

The board is ultimately responsible for the risk management and internal control framework but is likely to delegate various aspects of the monitoring and review activities to its committees and, most likely, to the audit committee.

One of the main roles and responsibilities of the audit committee under Provision 25 of the Code is to *'review the company's risk management and internal control framework, unless expressly addressed by a separate board risk committee composed of independent non-executive directors, or by the board itself'*.

Traditionally, audit committees oversaw risks related to financial reporting. In recent years, however, their role has extended to much more and, in many ways, is often considered more significant than that of other board committees. In fact, many are now designated as 'audit and risk committees'. This reflects that many principal risks can potentially impact the financial results and the viability of the business.

Nonetheless, oversight of certain principal risks can be allocated to specialised board committees. For example, a technology board committee might be tasked with overseeing cyber risk or a sustainability committee with climate change. In such cases, it is less clear which committee will have oversight of related material controls, and some boards may decide

that the audit committee remains best placed to do so. This is because audit committees typically:

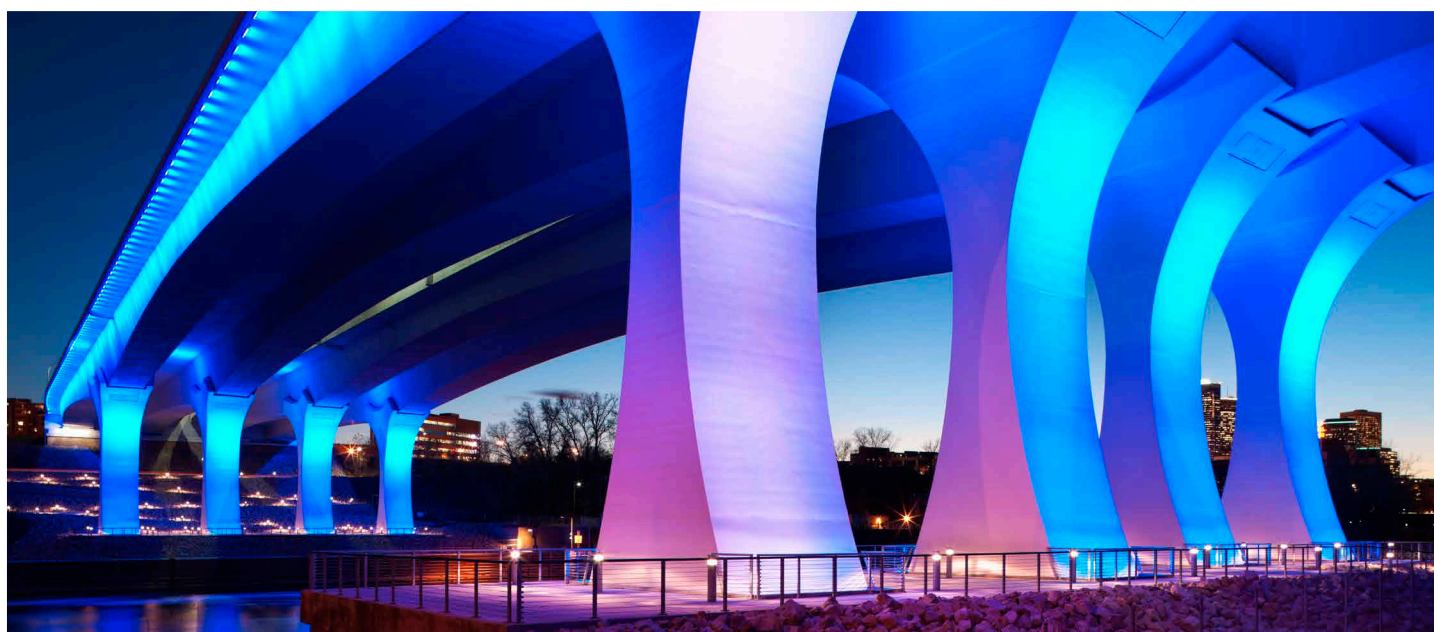
- ▶ Oversee internal controls over financial reporting and, therefore, are already familiar with entity-level controls that support them.
- ▶ Understand concepts such as control documentation, testing and assurance.
- ▶ Support the board with overseeing whistleblowing and similar matters.
- ▶ Monitor and review the effectiveness of the internal audit function as required by Provision 25 of the Code.

Furthermore, according to the FRC guidance, except to the extent expressly dealt with by the board or a risk committee, the audit committee should review and recommend to the board the disclosures included in the annual report in relation to risk management and internal control.

Regardless of how responsibilities are allocated, the board will have to act as the overall aggregator, and the declaration of controls effectiveness will ultimately be approved by the unitary board.

Other practical considerations

Review board and committee terms of reference to ensure clarity over responsibilities related to monitoring and reviewing the various aspects of risk management and internal controls framework, including oversight of the effectiveness of material controls.





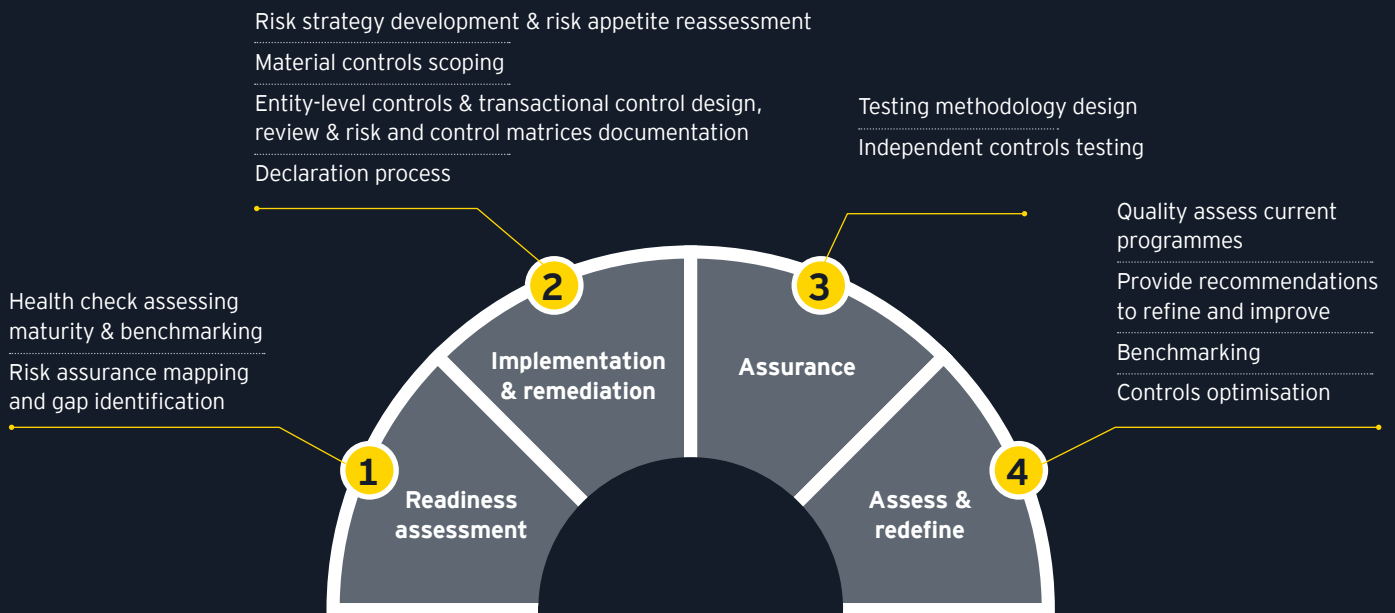
Given the broad scope of reporting regimes and laws and regulations cutting across the declaration, many organisations see Provision 29 as a catalyst for 'getting their house in order'.

Organisations find that revisiting and clearly documenting their overall approach to risk management is a useful starting point. We are supporting them in redefining and reshaping how they describe their principal risks and how they determine risk appetite.

We are also supporting organisations in defining what confidence and assurance mean for them and their boards. Testing conducted internally (usually through a clearly defined second line or independent third line) and by external third-party providers increases confidence. However, a robust controls self-assessment process may be appropriate in some cases. Performing comprehensive risk assurance mapping helps improve the overall understanding of the activities being conducted across the organisation and rethink existing testing strategies.

We support companies to assess the current roles and responsibilities within each line to help them achieve the right balance of activities, efficiently allowing the board to meet the requirements. For example, through our work, we have helped identify the following:

- ▶ Companies often designate their existing entity-level controls as material controls but do not challenge whether the documentation and testing of these controls need to be enhanced.
- ▶ Internal audit capacity in certain areas can be released and reallocated to other risk assurance needs. This is because internal and external assurance activities have been layered or duplicated over time.



For more information on how we support companies, please contact:



Neil Mathur
 Partner, Ernst & Young LLP
 Email: nmathur@uk.ey.com



Section 3

Enhancements to reporting

We are not setting a benchmark. Annual reports are for investors and stakeholders and should be used as an opportunity for additional engagement. Investors will want to consider the declaration in terms of the company and seek assurance that the board has appropriate oversight of the risk and internal controls framework.

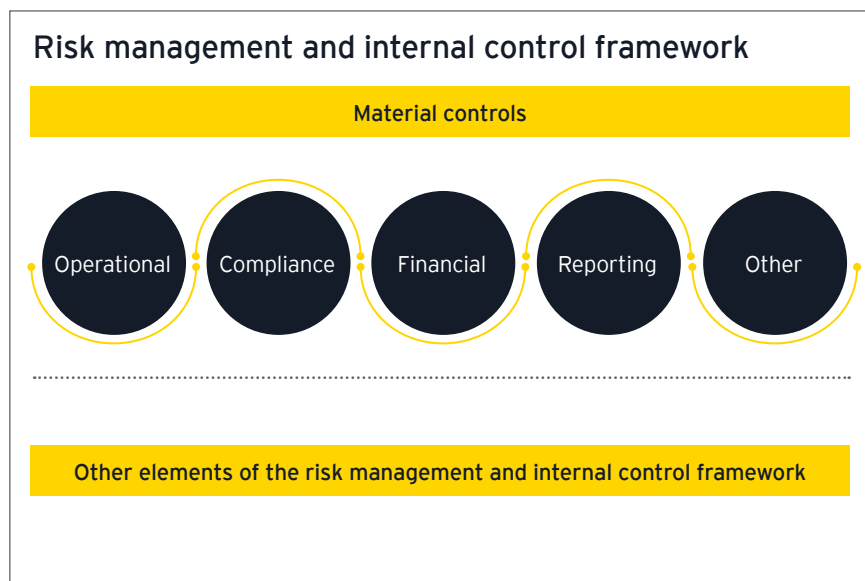
FRC Q&A

3.1. Overview

As noted before, Provision 29 introduces three specific reporting requirements:

1. A description of how the board has monitored and reviewed the effectiveness of the entire risk management and internal control framework (which includes material controls)
2. A declaration of effectiveness of the material controls as at the balance sheet date
3. A description of any material controls that have not operated effectively as at the balance sheet date, the action taken or proposed to improve them and any action taken to address previously reported issues

- ▶ Make a declaration of effectiveness as at balance sheet date.
- ▶ Describe which, if any, material controls had not operated effectively as at the balance sheet date and the action (taken/proposed) to improve them.
- ▶ Describe any action regarding previously reported issues.



- ▶ Monitor and at least annually review.
- ▶ Describe how this has been done.

Most of the reporting in the updated Provision 29 is already required by the 2018 Code or recommended by the related guidance. Therefore, companies currently disclose many aspects but may need to review and reconsider the completeness, order and specificity of their current disclosure. We set out our recommendations based on observations from current reporting.

3.2. Re-ordering the flow

Whilst much focus has been on making the declaration within Provision 29 it cannot be made in isolation from other linked disclosures within the annual report. Most annual reports voluntarily disclose information on the main features of the risk management and internal control framework. This is typically spread between a section of the strategic report, often titled 'risk management' or 'principal risks and uncertainties', and the 'governance section' – most commonly in the audit (and risk) committee's report.

However, practice varies greatly, and content is not always easy to locate. For example, the board's confirmation that it has carried out a robust assessment of the company's emerging and principal risks can be included as part of the principal risk disclosure, the overall governance statement, the audit committee's report and sometimes the viability statement.

Similarly, it is fairly common for the audit committee's report to describe elements of the risk management and internal control framework, either duplicating the earlier 'risk management' section or providing some new information, e.g., on the set-up of the Internal Audit function or even on the

control framework and how management monitors and tests the controls.

As the FRC has not dictated how companies should report, companies will need to consider how best to restructure the narrative's overall flow.

We are advocating for a logical flow that:

- ▶ Starts with a description of the risk management and internal control framework
- ▶ Sets out the activities undertaken by various levels within the organisation
- ▶ Leads to outcomes-based governance reporting that explains how the board monitored and reviewed the framework
- ▶ Culminates in the declaration of material controls effectiveness

Recommendation

Consolidate all the risk management and internal controls framework descriptions within the strategic report into one comprehensive disclosure. This will also help delineate the narrative in the governance section, which should detail how the board and its committees monitored and reviewed the framework's effectiveness.

The structure of this section

The graphic below shows how the rest of this section has been structured. We cover the following:

- ▶ What good reporting on management activities looks like
- ▶ The governance reporting that follows on from that

What management does

3.3 Risk management and internal control framework

Risk management process

Internal control framework

3.4 Principal risk disclosure

Mitigating actions

Additional attributes

What the board does

3.5.2 Good practice governance reporting

Board-level monitoring

Board-level review

Risk management process

Principal and emerging risks

Internal controls and other mitigating actions

Outcomes

Conclusions



3.3. Risk management and internal control framework

The board should describe the main features of the [risk management and internal control] framework, including an overview of the relevant governance structures in place, how the company assesses risks, how it manages or mitigates them, and how information is shared throughout the organisation and how different units interact and communicate.

FRC guidance, para 293

3.3.1. Risk management process

The majority of companies include an overview of their risk management process, typically setting out with varying degrees of detail the following:

- ▶ Governance structure (e.g., [Rio Tinto 2023 ARA, p. 79](#))
- ▶ Risk management roles across the three lines (e.g., [The Weir Group 2023 ARA, p. 63](#))

- ▶ Steps in the process, such as risk identification, prioritisation/analysis, evaluation, risk responses, monitoring and assurance (e.g., [Tesco 2024 ARA, pp. 30-31](#))

Better reporters:

- ▶ Explain whether emerging risk identification differs from that of principal risks. Whilst more companies define and explain their emerging risks and how they are assessed, not all explain whether their identification differs from that of principal risks. Companies commonly refer to horizon scanning, but unlike [Lloyds Banking Group \(2023 ARA, pp. 44, 144\)](#), they seldom describe what horizon scanning actually entails.
- ▶ Provide clarity on the delegation of responsibilities from the board to its committees and set out the top-down and bottom-up procedures for identifying risks, as done by [Croda \(2023 ARA, p. 52\)](#).
- ▶ Explain what is taken into account when risks are monitored and assessed across different layers of the organisation, as done by [SThree \(2023 ARA, p. 76\)](#).

Recommendation

When providing an overview of the governance structure, be precise about which board committee oversees which risk. When setting out steps in the risk management process, consider including board-level monitoring as an explicit element, given the requirement to disclose how the board monitored the risk management framework.



3.3.2. Internal control framework

Generally, comprehensive disclosures on internal control are less common than those related to risk management. Companies that share more insights do this in the following ways:

- ▶ Expand their three-lines model and identify the responsibilities each line has in respect of controls and the associated monitoring of their operational effectiveness (e.g., [Reckitt 2023 ARA, p. 94](#)).
- ▶ Provide a standalone disclosure that describes the tiers of controls that form part of the framework. For example:
 - ▶ [The Weir Group \(2023 ARA, p. 90\)](#) explains what forms part of its four tiers of controls.
 - ▶ [BAE Systems \(2023 ARA, p. 87\)](#) sets out an operational framework listing key policies.
 - ▶ [3i Group \(2024 ARA, p. 127\)](#) includes a summary of its key control framework.
- ▶ Detail internal financial controls, in line with DTR 7.2.5's requirement to provide a "description of the main features of the issuer's internal control and risk management systems in relation to the financial reporting process" (e.g., [Derwent London 2023 ARA, p. 149](#)).

There is no requirement to include a list of controls identified as material by the board, nor does the board's declaration need to indicate the number of material controls it covers. However, companies that do not already explain the features of their internal control system may need to enhance their reporting to allow a reader to understand the positioning of material controls within that context.

Recommendation

Describe the tiers of internal controls within the organisation. Explain how material controls have been defined against that backdrop, including how materiality was interpreted. In the first year, consider explaining how the initial list of material controls covered by the board's declaration was identified.

Some companies also explain how they obtain confidence that internal controls are operating as intended by:

- ▶ Describing control self-assessment processes in place (e.g., [Intertek Group 2023 ARA, p. 76](#))
- ▶ Setting out the approach to second-line controls testing (e.g., [Serco Group 2023 ARA, p. 33](#))
- ▶ Specifying exactly what work is undertaken by Internal Audit in relation to internal controls (e.g., [Beazley 2023 ARA, p. 117](#))

Recommendation

Consider explaining and contrasting the roles and responsibilities across the three lines, for example, in a tabular format, as shown below. Even if not provided as a disclosure in the annual report, this clarity should exist in internal documentation.

Reporting line	First line	Second line	Internal audit
Role in respect of risk management			
▶ Principal risks			
▶ Emerging risks			
▶ Risk registers			
Role in respect of internal control			
▶ Activities (e.g., self-certification, testing)			
▶ Scope (including in respect of disclosures)			
▶ Level of confidence (e.g., limited assurance)			
Formal reporting			

3.4. Principal risk disclosure

On average, companies disclose 11 principal risks, with 10 being the most common; a minority disclose more than 16 or fewer than seven. Very few companies include a disclosure-related principal risk. As part of this process, boards may wish to consider whether to do so.

Provision 28 of the Code continues to require a description of principal risks and how these are managed and mitigated. Most commonly, companies have a tabular disclosure with a column explaining the risk and its impact and a separate column setting out the related mitigations, some of which are controls (or can be inferred as such).

3.4.1. Mitigating actions

Although there is no requirement to disclose material controls, companies should be mindful that readers may interpret or infer controls disclosed within mitigating actions to be material controls.

Interestingly, although more than three-quarters of companies disclose a year-on-year change in overall risk profile, less than a third of these disclose how mitigating actions evolved as a result. Such insight would demonstrate the dynamism of risk management and governance outcomes.

In addition, just over a third of companies refer to assurance processes as part of discussing mitigating actions for a subset of their principal risks, most commonly health and safety, cybersecurity or regulatory compliance. These references are typically high-level and often do not go as far as specifying whether the assurance is internal or external. A few companies, like [Rolls Royce Holdings \(2023 ARA, p. 52\)](#) and [IHG \(2023 ARA, p. 46\)](#), provide this disclosure against all principal risks. Rolls Royce Holdings discloses assurance activities and providers, and IHG summarises the internal audit plan's considerations.

Recommendation

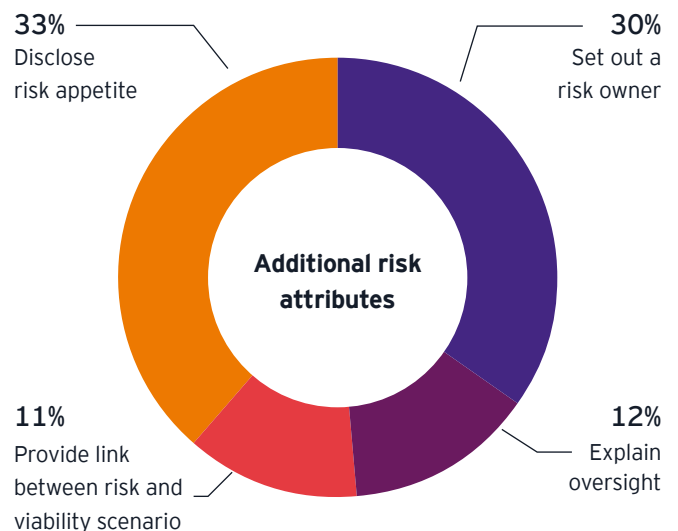
Provide an example of a material control against relevant principal risks – on the one hand, this will bring the concept to life, and, on the other, clarify that any other controls that have been listed are not material controls. Where there has been a change (increase) in risk profile, clarify whether incremental processes were put in place, including if any new material control(s) had been designated during the year in response.

Consider disclosing assurance activities against each principal risk, as this would be more meaningful than a summary within the description of the board's monitoring and review activities.

3.4.2. Additional risk attributes

Practice varies greatly on what additional risk attributes are disclosed, with a few companies setting out risk velocity, time period and interconnectivity. Including the following attributes can support reporting against Provision 29:

- ▶ Set out a risk owner – done by around 30% of companies, including e.g., [Pearson \(2023 ARA, p. 63\)](#).
- ▶ Explain which governance body has oversight of that particular risk – done clearly by around 12% of companies, including [Glencore \(2023 ARA, p. 106\)](#).
- ▶ Provide a link between the risk and any related viability scenario. Around 11% of companies, including [Rotork \(2023 ARA, p. 74\)](#), do this. This is useful because not every principal risk needs to be managed or mitigated to the same extent, and boards may decide that, for example, controls in respect of principal risks not included within viability statement scenarios do not meet the definition of a material control or that principal risks with a high risk appetite require fewer material controls than those where the risk appetite is low.
- ▶ Disclose the risk appetite – around a third of companies provide a risk appetite rating (e.g., [Balfour Beatty 2023 ARA, p. 94](#)) or a specific risk appetite statement for each principal risk (e.g., [Computacenter 2023 ARA, p. 69](#); [BT Group 2024 ARA, p. 63](#)). Additionally, a few state whether the risk had remained within the risk appetite (e.g., [RHI Magnesita 2023 ARA, p. 52](#)).



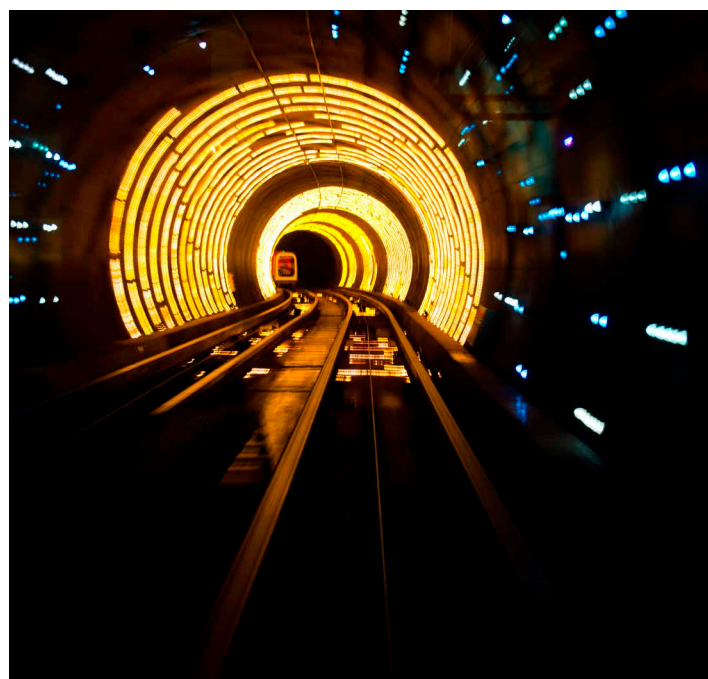
Recommendation

When disclosing principal risks, consider disclosing additional risk attributes that explain the focus of the board's monitoring and review activities.

3.5. Reporting on governance activities

The board should provide a summary of how it has monitored and reviewed the effectiveness of the framework during the reporting period. This may include the type of information the board has received and reviewed; the units and individuals it has consulted with; any internal or external assurance received (...)

FRC guidance, para 294



The quality of governance reporting on directors' oversight of the risk management and internal control framework varies considerably. The narrative is typically included within the audit committee report (and risk committee report, where relevant).

Whilst there are pockets of good practice, overall, the disclosures will need to evolve to provide a meaningful basis for the directors' material controls declaration and be outcomes-focused.

3.5.1. Aspects of current practice that will need to evolve

Not surprisingly, given current requirements, the governance narrative is often limited to confirming that a review of the risk management and internal control framework took place. The confirmation that a robust assessment of risks had been completed is included separately.

In many cases, little to no detail is included about what the review and assessment entailed; however, an illusion of length and depth of content is created by inserting the following:

- ▶ Boilerplate statements about the framework being designed to manage rather than eliminate risk.
- ▶ Statements about the delegation of authority from the board to the audit committee, something typically already included within disclosures of the overall governance structures.
- ▶ An explanation of the internal control framework's key elements, often focusing on controls over financial reporting – whilst this information is meaningful, it does not relate to governance activities.

Companies that go a step further include a list of the responsibilities delegated to the audit committee. However, this can be quite generic and written in the present tense, making it hard for the reader to understand what specific activities were actually undertaken during the year.

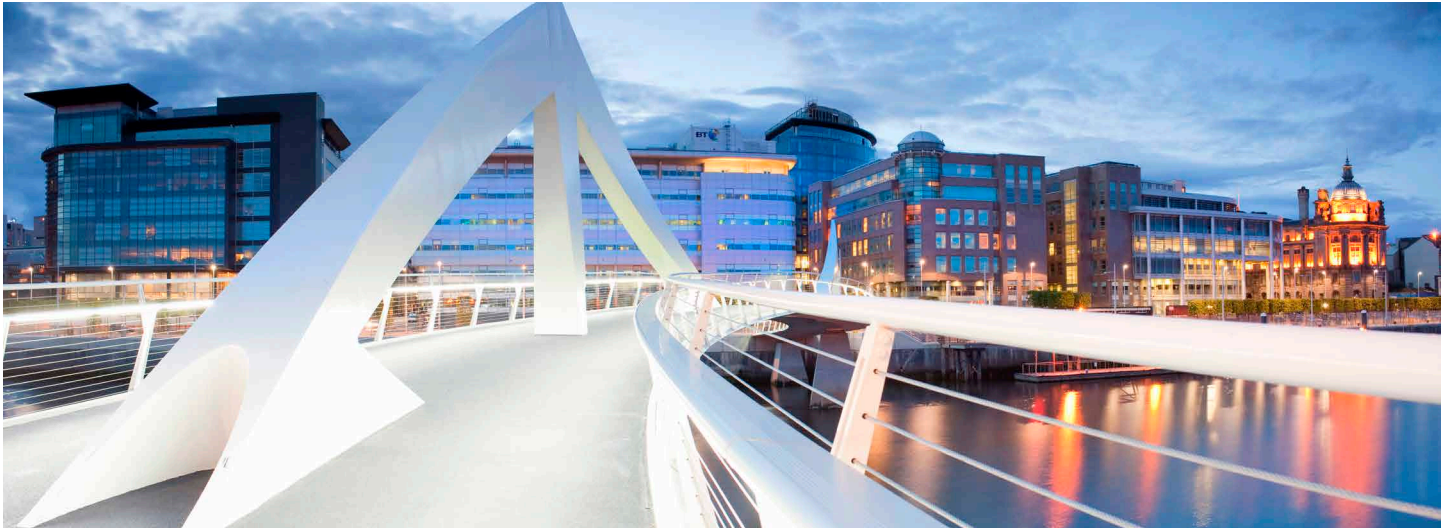
3.5.1.1. Reports and presentations

Some companies map the remit of their governance bodies against topics on which they received reports. This provides some insight; however, the language used is often passive – *'the audit committee was updated, it received reports ...'*. When more active phrases like – *'the audit committee discussed the report ...'* are used, the reader is seldom informed who it was discussed with. Alternatively, some companies set out from whom the audit committee received reports but not on what topics. Often, it is also unclear whether the author/owner of the report attended the audit committee meeting to respond to any questions.

In either case, it is uncommon for the narrative to explain what actions the audit committee took after receiving a report, including whether it requested additional information or how this may have influenced its priorities for the year ahead.

3.5.1.2. Cadence of monitoring activities

To bring out the ongoing nature of the audit committee's involvement, the narrative sometimes refers to the audit committee receiving 'regular reports'. However, it is more meaningful to use precise terms such as 'quarterly reports' or 'presentations twice a year'. Another means through



which companies demonstrate frequency is by disclosing key activities by meeting. It is generally more helpful to demonstrate the cadence of monitoring the risk management and internal control framework if the activities of the audit committee are grouped (e.g., [BT Group 2024 ARA, p. 100](#)) or colour-coded thematically. Alternatively, some companies include a standalone disclosure related to those aspects of monitoring (e.g., [Inchcape 2023 ARA, p. 63](#); [John Wood Group 2023 ARA, p. 83](#))

Detailing the ongoing monitoring that supports the board's review at year-end is important, as currently, narratives either refer to monitoring and review interchangeably or focus only on the review element. This is not surprising, as monitoring is typically associated with management activities. Companies will need to demonstrate the board-level monitoring activities and whether they led to any actions to strengthen the risk management and internal control framework, e.g., evolving mitigating actions in response to changes in risk profile or overseeing remediation when 'near misses' were identified in respect of material controls.

3.5.1.3. Oversight of internal controls

Generally, governance reporting includes more information about activities undertaken for risk-related aspects than internal control. To an extent, this is influenced by the fact that financial services companies have standalone risk committees that focus on this aspect. However, because only around 37% of companies separate the reporting related to risk from that related to internal control, it is often difficult to distinguish what work has actually been undertaken to monitor and review the operation of internal controls. This is exacerbated by the fact that the audit committee narrative in respect of internal control often refers only to controls over financial reporting. Oversight of other controls (relating to non-financial disclosures or business risks) is not addressed elsewhere in the annual report.

Provision 25 of the 2018 Code included the following as one of the main roles and responsibilities of the audit committee: 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.

In the 2024 Code, this has been replaced with: *reviewing the company's risk management and internal control framework, unless expressly addressed by a separate board risk committee composed of independent non-executive directors, or by the board itself.*

Thus, the focus on controls over financial reporting has been removed. However, paragraph 225 of the supporting guidance does state that, *the audit committee should review the company's internal financial controls, that is, the systems established to identify, assess, manage and monitor financial risks, as part of its expected roles and responsibilities in the Code.*

3.5.1.4. Sources of confidence

The largest gap to address in governance reporting relates to providing clarity on the robustness of the declaration. As there is no requirement for any form of assurance over the declaration, one of the aims of detailing the review and monitoring process is to offer transparency to readers regarding the basis on which directors have concluded the effectiveness of material controls. The narrative will, therefore, need to become much clearer in explaining the sources of confidence directors obtained by reference to the lines of defence and any external providers.

3.5.2. Good practice governance reporting

Monitoring and review, as well as risk management and internal controls, are intrinsically linked, and we are not advocating that the oversight narrative be distinctly split across these topics. However, companies will need to ensure that all of these matters have been given due consideration and can be easily identified, with the following covered at a minimum:



	Monitoring		Review		
	Provision 29 How	Principle C	Provision 29 How	Provisions 28 and 29	Provision 29 How
	Activities and their frequency	Outcomes/ actions taken	Activities	Conclusions	Sources and level of confidence
Risk management process	x	x	x		
Emerging risks			x	Provision 28 confirmation	
Principal risks			x	Provision 28 confirmation	
Principal and other risk mitigations including controls	x	x	x	Provision 29 – for material controls	x
Controls over disclosures	x	x	x	Provision 29 – for material controls	x

Properly addressing Provision 29 requires reporting on how the board conducted the monitoring and review. This is the basis for the material controls effectiveness declaration. As there is no presumption that the scope of monitoring overlaps completely with the scope of the review, companies will need to explain what is in fact monitored by directors on an ongoing basis and what was reviewed.

Companies may find the following examples of good practice helpful when enhancing the governance narrative to meet this higher standard of transparency.

3.5.2.1. General (refer to [Figure 27](#) for extracts)

- ▶ When referring to reports received by the board, be clear on the report's topic and who it was from (e.g., [Rentokil Initial 2023 ARA, p. 123](#)).
- ▶ Provide some detail on what was included in the report and what factors were considered as part of the review (e.g., [Legal & General Group, 2023 ARA, p. 93](#); [Severn Trent 2023 ARA, p. 157](#)).
- ▶ Demonstrate how various inputs and sources were used to challenge management's conclusions (e.g., [The Weir Group 2023 ARA, p. 101](#)).
- ▶ Be clear on any external sources/inputs used in making assessments, such as benchmarking or publications from professional bodies and institutions (e.g., [PPHE Hotel Group 2023 ARA, p. 127](#)).

- ▶ Include reference to activities undertaken after year-end in so far as they relate to assessments as at the year-end (e.g., [Whitbread 2024 ARA, p. 121](#)).

3.5.2.2. Risk and risk management-related

(refer to [Figure 30](#) for extracts)

Overall, reporting on risk oversight is more in-depth in companies with a risk committee. For example, in its 2023 [ARA \(pp. 102-106\)](#), [Lloyds Banking Group](#) includes a table disclosing each risk, the key issues, what the risk committee reviewed and its conclusions.

Other considerations include:

- ▶ Explain which risk attributes were considered in conducting assessments (e.g., [SThree 2023 ARA, p. 76](#)).
- ▶ Be explicit about which risk events or changes to external factors influenced risk deliberations (e.g., [Morgan Sindall Group 2023 ARA, p. 128](#)).
- ▶ Clarify what actions were taken when the risk profile for a principal risk increased. For example, [AstraZeneca \(2023 ARA, p. 95\)](#) notes spending additional time on risks relating to IT, cyber risk and data security, and [Drax Group \(2023 ARA, p. 95\)](#) refers to an enhancement in the level of assurance obtained given increased risk.
- ▶ Be specific about the work undertaken by Internal Audit for particular risks in a given year (e.g., [Smith+Nephew 2023 ARA, p. 117](#)). This can also be facilitated by setting out those activities as part of the principal risk disclosure (e.g., [IHG 2023 ARA, p. 46](#)).

3.5.2.3. Controls-related (refer to [Figure 31](#) for extracts)

- ▶ Explain the process used to assess material controls, including actions undertaken if weaknesses are identified (e.g., [Lloyds Banking Group 2023 ARA, p. 93](#))
- ▶ Set out how directors were kept abreast of any near misses (e.g., [NatWest 2023 ARA, p. 111](#))
- ▶ Be clear about any areas of improvement that were identified, actions taken as a result (e.g., [Taylor Wimpey 2023 ARA, p. 122](#)), and updates on remediation status (e.g., [bp 2023 ARA, p. 102](#))
- ▶ Reference the role played by directors in overseeing controls transformation programmes (e.g., [Ocado Group 2023 ARA, p. 150](#))
- ▶ Explain the board's conclusion, taking account of any areas of weakness and plans for improvement (e.g., [Persimmon 2023 ARA, p. 113](#))

3.5.2.4. Level of confidence (refer to [Figure 32](#) for extracts)

- ▶ Clarify the board's sources of assurance and how they are adequate to give the board confidence. Some companies (e.g., [Drax Group 2023 ARA, p. 95](#)) refer to assurance maps and how their adequacy was challenged.
- ▶ Be clear whether directors reviewed the results of any self-attestation or second-line testing that had been performed (e.g., [Convatec Group 2023 ARA, p. 115](#); [Phoenix Group Holdings 2023 ARA, p. 97](#)).
- ▶ State whether internal audit work specifically addresses the effectiveness of controls (e.g., [Howdens 2023 ARA, p. 139](#); [Morgan Sindall Group 2023 ARA, p. 129](#)).
- ▶ Be specific about changes to the scope of assurance sought during the year, including from internal audit (e.g., [Travis Perkins 2023 ARA, p. 104](#)).

3.6. The declaration

The declaration relates to the effectiveness of material controls as at the balance sheet date, not the effectiveness of the overall risk management and internal control framework. There is no template for this declaration, but as long as its basis is clear (as discussed in the rest of this section), it can be as brief as stating:

The board confirms that it has monitored the risk management and internal control framework throughout the year. It is satisfied that, at the time of conducting the year-end review, any significant failings or weaknesses related to material controls identified as part of the monitoring had been adequately remediated. The year-end review provided the board with sufficient appropriate evidence and reasonable confidence to determine that all material controls were effective as at the balance sheet date.

3.6.1. Reporting ineffectiveness

Where relevant, directors are required to describe any material controls that have not operated effectively as at the balance sheet date, alongside actions taken or planned to improve them. There is no guidance on the level of detail required when describing the ineffective material controls, but the disclosure should enable the reader to understand the control's objectives. Material controls may be very company-specific, requiring a more granular description than provided in disclosing material weaknesses under US SOX.

Whilst not required, we recommend including the expected timeline for implementing remedial actions to demonstrate that an action plan is in place.

Any actions taken to address previously reported issues must also be set out. When reporting on these areas, the board is not expected to provide disclosures that, in its professional judgement, contain confidential information or any other information that could inadvertently affect the company's interests if publicly reported.

3.6.2. Providing explanations

If the board could not determine the effectiveness of any material controls or material controls over certain areas, reporting the explanation should follow Principle C of the Code. In the introduction to the Code, the FRC explains that: *Explanations should set out the background, provide a clear rationale for the action the company is taking and explain the impact that the action has had. Where a departure from a Provision is intended to be limited in time, the explanation should indicate when the company expects to conform to the Provision.*

We would not expect companies to explain against the requirement to disclose how monitoring and review were performed.

Recommendations

- ▶ Include the declaration within the overall governance statement, not within one of the board committee reports
- ▶ Consider combining this with the statement required by Provision 28 with respect to conducting a robust assessment of emerging and principal risks
- ▶ Precede the declaration with an explanation of how the board, as a whole, was involved in the monitoring and review activities
- ▶ Provide a cross-reference to those committee reports that undertook aspects of the monitoring and review of the risk management and internal control framework

Section 4

Next steps

The intentional flexibility afforded by the Code will inevitably lead to different approaches to implementation, particularly in the initial years. Directors who serve on multiple boards may receive different proposals from their respective management teams. Early engagement between boards and management is critical to prevent any divergence in expectations and avoid surprises.

As a first step in preparing to meet the new requirements, boards may wish to revisit the existing activities related to monitoring and reviewing the risk management and internal control framework to decide what they should continue to leverage and where most attention is needed. We also recommend using the two upcoming reporting cycles to gradually evolve disclosures in the annual report in readiness for the first reporting in 2026-27.

Below, we have set out next steps against an indicative timeline in the lead up to the first year of compliance with Provision 29¹. We recognise that companies will be at different stages of preparation and maturity and, hence, will progress at different speeds.



No later than the end of FY24

- ▶ Establish a cross-functional management steering committee responsible for developing the approach to meeting the requirements of Provision 29 on behalf of the board
- ▶ Agree the definition of material controls
- ▶ Determine which disclosures will require material controls
- ▶ Determine which (principal) risks will require material controls
- ▶ Walkthrough: For one principal risk, present to the board a proposal for:
 - ▶ The related material controls
 - ▶ How they will be documented
 - ▶ The criteria to determine their effectiveness
 - ▶ Thresholds for near misses reporting
 - ▶ The reporting to be received by the board on the operation of the material controls to allow for board-level monitoring and review
 - ▶ The sources and levels of confidence to help the board make its declaration
- ▶ Use this to align on the board's expectations and agree an approach to other risk areas

1. Dates by reference to companies with a 31 December financial year end



In your FY24 annual report

- ▶ Re-order existing disclosure to streamline and consolidate content in the most relevant sections
- ▶ Streamline and improve the precision of terms used
- ▶ Augment existing disclosures so that they are fully reflective of current practices
- ▶ Stand back and assess whether the description of monitoring and review activities will give readers confidence in the basis for future declaration

No later than the first half of FY25

- ▶ Establish an initial list of material controls (over disclosures and risks) approved by the board, including criteria to determine their effectiveness
- ▶ Assign ownership and oversight for each material control
- ▶ Agree upon a target level of confidence required for each material control
- ▶ Outline the existing activities undertaken to assess the effectiveness of each material control and identify any steps needed to reach the target level of confidence
- ▶ Agree the cadence for monitoring, including what is presented to the board (e.g., data points, evidence, assurance results)

No later than the second half of FY25

- ▶ Conduct a dry run for all material controls and identify any weaknesses that could result in a material control not operating effectively at the year-end
- ▶ Reassess whether the reporting received by the board and the target confidence levels remain appropriate
- ▶ Discuss whether any material controls may need to be scoped out of the declaration and an explanation provided
- ▶ Agree the board's appetite for disclosing any material controls' ineffectiveness and actions required to address identified weaknesses
- ▶ Review and update the initial list of material controls; changes could occur due to increase/decrease in risk appetite, new risks etc
- ▶ Prepare a private, internal use draft of the material controls declaration including any ineffectiveness explanations

In your FY25 annual report

- ▶ Create full disclosure of risk management and internal control framework
- ▶ Use precise language that accurately reflects any testing and assurance activities
- ▶ Provide a fulsome monitoring and review narrative, reflecting any changes to the processes implemented in FY25
- ▶ Ensure that outcomes of the board's monitoring are disclosed, given Principle C will already be applicable
- ▶ Consider trailing externally any areas where you may need to 'explain' rather than comply in FY26



Appendix: Illustrative examples

Illustrative examples for 3.3.1 Risk management process

Figure 1

Rio Tinto 2023 ARA, p. 79 – Setting out the governance structure

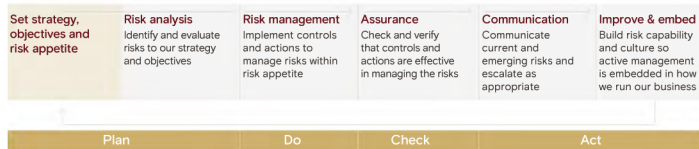
Our approach to risk management

To protect and create value, we aim to have the right people at the right level managing risks.

Our risk management, values and risk appetite inform and shape our risk management framework. We embed risk management at every level of the organisation to effectively manage threats and opportunities to our business and host communities, and our impact on nature.

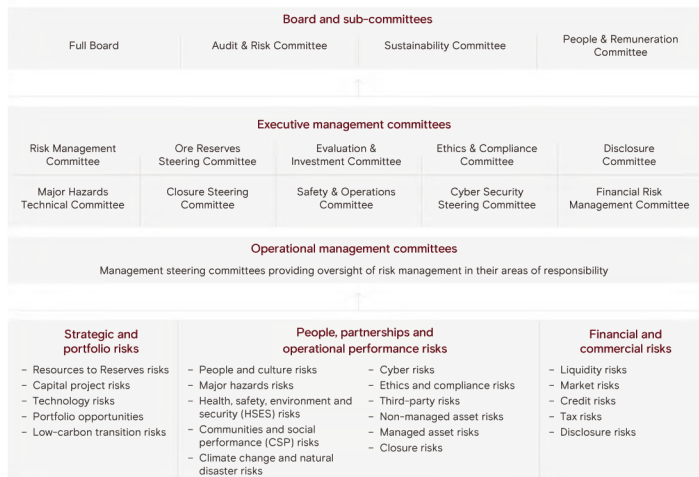
Our risk management process can be described as a Plan-Do-Check-Act cycle. We monitor how well we manage material risks to our objectives by checking and verifying the implementation of our response plans (actions and controls) and our actual performance against objectives. We enhance the check-and-verify step by applying the three lines of defence approach.

Our risk management process



Rio Tinto has an enterprise-wide risk management information system (RMIS) which includes a set of integrated tools and applications to capture, manage and communicate material risks to the business. We are currently implementing a program to refresh our three lines of defence as a core part of the risk management framework, enabled by the development and implementation of a Group Control Library to strengthen the first line and optimise the second line.

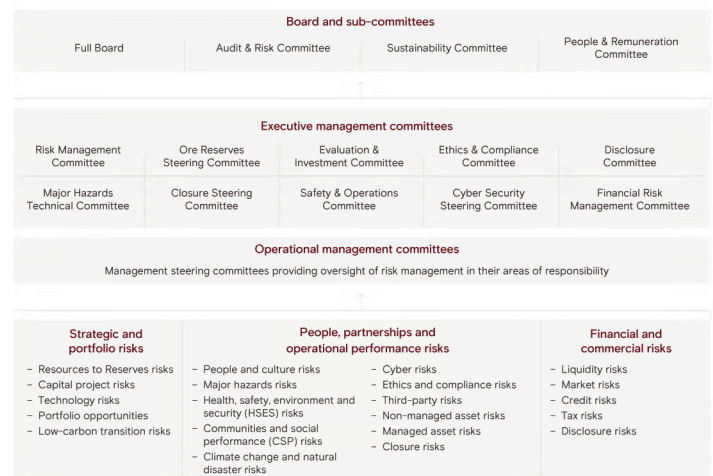
Governance structure supporting our risk management framework



The Board and the Executive Committee oversee our principal risks, and the Audit & Risk Committee monitors the overall effectiveness of our risk management and internal controls framework. In addition, the operational management committees of our product groups and Group functions also oversee risk management in their area of responsibility, with insights from assurance and compliance activities.

At the front-line operational level, all employees are required and empowered to own and manage the risks that arise within their area of responsibility. This governance structure supports our risk management framework and enables effective management of material risks.

Governance structure supporting our risk management framework



Source: <https://cdn-rio.dataweavers.io/-/media/content/documents/invest/reports/annual-reports/rt-annual-report-2023.pdf?rev=8290537a1f0047888ae79319753a3ec4>

Figure 2

The Weir Group 2023 ARA, p. 63 – Explaining risk management roles across the three lines

Risk management

continued

Risk management roles and responsibilities

The key roles and responsibilities for risk management are set out below.

	Group	Risk management responsibilities
THIRD LINE OF DEFENCE	Board Overall responsibility for the Group's risk management and internal control frameworks, and strategic decision within the Group.	<ul style="list-style-type: none"> Annual review and ongoing monitoring of the effectiveness of the risk management and internal control frameworks. Annual review of the Group's risk appetite. Assessment of the Group's principal and emerging risks. Twice a year receive a report from the Risk Committee that sets out the current assessment of each principal risk, the effect of mitigating controls on each risk, the direction of travel of each risk versus the prior year, the extent to which each could potentially impact the Group's strategic goals and any relevant findings relating to significant control failings or weaknesses which have been identified. Taking decisions in accordance with the delegated authority matrices.
	Audit Committee Delegated responsibility from the Board to review the effectiveness of the Group's risk management and internal control frameworks.	<ul style="list-style-type: none"> Annual assessment of the effectiveness of the risk management and internal control frameworks. Review of reports from management and internal and external auditors. Review of the results from the six-monthly self-assessment compliance scorecards.
	Group Executive Executive committee with overall responsibility for managing the Group to ensure it achieves its strategic objectives.	<ul style="list-style-type: none"> Managing risks that have the potential to impact the delivery of the Group's strategic objectives. Monitoring business performance, in particular, key performance indicators relating to strategic objectives. Taking strategic decisions in accordance with the delegated authority matrices. Escalating issues to the Board as required.
SECOND LINE OF DEFENCE	Risk Committee Management committee responsible for governance of the Group's Risk Management Policy and framework.	<ul style="list-style-type: none"> Review of the design and operation of the Group's Risk Management Policy and framework. Identification and assessment of the key risks facing the Group, identification of the key controls mitigating those risks and identification of further actions where necessary. Identification and review of emerging risks and opportunities Review of the Divisional risk dashboards, considering the appropriateness of management's responses to identified risks and assessing whether there are any gaps. Reporting key Group and Divisional risks to the Board.
	Chief Executive's Safety Committee Safety committee with responsibility to set and monitor the Group's SHE principles, priorities and actions.	<ul style="list-style-type: none"> Executive Committee representation to drive improvements in our safety performance throughout the Group. Champion the Group's Safety, Health and Environmental (SHE) Charter, reinforcing our commitment to maintaining a zero harm workplace. Ensure the strategy for SHE improvements is comprehensive, risk-based, deliverable and balanced and built on best practice from peers, customers and suppliers.
	Management Committees Several management-led committees, some of which are known as Excellence Committees. These committees cover a wide range of subject areas relevant to the Group and delivery of its strategy objectives including safety, sustainability, technology, and inclusion, diversity and equity.	<ul style="list-style-type: none"> Monitoring the management of key risks across the Group associated with the respective remits of the Management Committees. Monitoring performance and compliance with Group objectives, policies and standards related to the respective remits of the Management Committees. Taking decisions in accordance with the delegated authority matrices. Escalating issues to the Group Executive as required. Reviewing the results from relevant assurance activities. Design and administration of the Group's compliance programme covering core areas including anti-bribery, anti-corruption, anti-trust, privacy, trade controls and human rights.
	Divisional management Responsible for managing the businesses within the Divisions to ensure Divisional strategic objectives are achieved and there is compliance with Group policies and standards throughout their Division.	<ul style="list-style-type: none"> Identifying and managing risks that have the potential to impact the delivery of the Division's strategic objectives. Monitoring performance and compliance with Group objectives, policies and standards within the Divisions and with regard to the outputs from the Excellence Committees. Taking decisions in accordance with the delegated authority matrices. Escalating issues to the Group Executive as required. Reviewing the results from relevant assurance activities.
FIRST LINE OF DEFENCE	Operating company management Responsible for ensuring company objectives are achieved and business activities are conducted in accordance with Group policies and standards.	<ul style="list-style-type: none"> Identifying and managing risks that have the potential to impact the delivery of their company's strategic objectives. Monitoring performance and compliance with Group objectives, policies and standards within their company. Taking decisions in accordance with the delegated authority matrices. Escalating issues to Divisional management and Excellence Committees as required. Reviewing the results from relevant assurance activities.

Source: <https://www.global.weir/siteassets/pdfs/2023-annual-report/weir-group-2023-annual-report.pdf>

Figure 3

Tesco 2024 ARA, pp. 30-31 – Steps in the risk management process

Principal risks and uncertainties

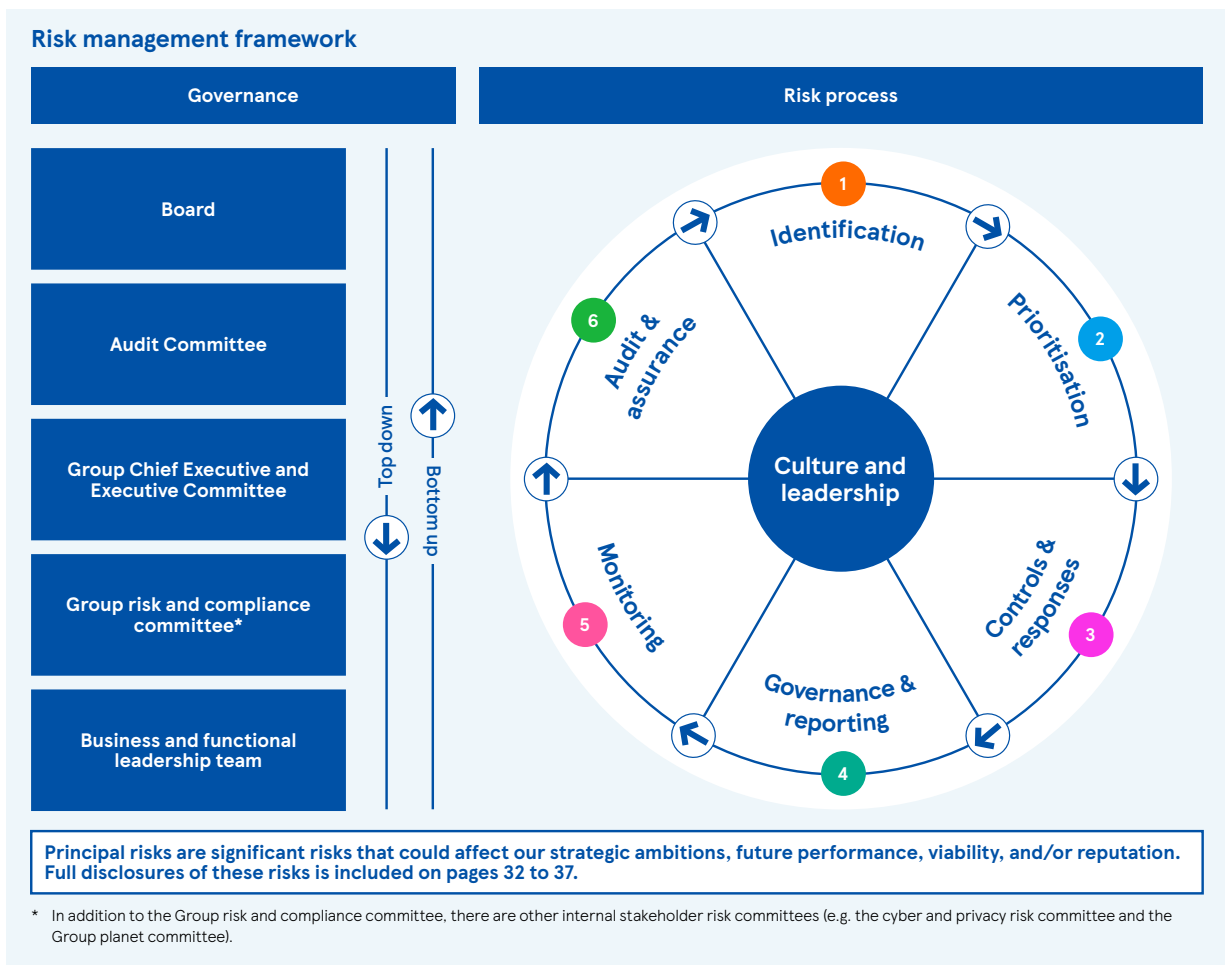
Managing our risks.

Effective risk management is core to our management practices which help deliver our strategy and our commitments to our customers, community, and the planet. We are focused on conducting our business responsibly, safely, and legally, while making risk-informed decisions when responding to opportunities or threats that present themselves. The Board and Executive Committee are responsible for the effective management of risk across the Group and we manage our risks in line with the risk appetite set by the Board.

Risk management framework (RMF)

The diagram below provides an overview of our framework defining Tesco's risk management process and governance. Our RMF continues to

be embedded throughout the organisation, enabling us to clearly identify, prioritise, respond, and monitor our most significant risks and emerging risk themes. Our RMF supports decision making, with culture and leadership being at the heart of our framework, including a clear tone from the top on the importance of risk management. Our colleagues play a vital role in carrying our culture forward through their commitment to our shared values on risk management. We provide regular learning opportunities to strengthen our colleague awareness on various risks and controls, for example providing appropriate training to help prevent cyber security incidents, as well as communicating the opportunities and safeguards while using artificial intelligence tools.



We are cognisant of the revised UK Corporate Governance Code requirements set by the FRC and have appropriate plans in place.

Risk identification and prioritisation

A complete view of our risk universe starts with the analysis of our business, the external environment within which we operate, the regulatory landscape and our internal operations. This includes the impacts on our strategy, initiatives, governance and processes. We use a consistent assessment criterion to identify and prioritise risks at the Group, business unit and functional level, along with horizon scanning for emerging risk themes. The identified risks are categorised into one or more of the following risk types: strategic, change, operational, finance or compliance. This enables effective governance and monitoring of the risks.

Management assesses the risks on a continuous basis, taking into account the risk to Tesco's strategy, our colleagues and our operations, as well as our impact on society and the environment. There is regular formal oversight through clearly defined governance structures, e.g. the cyber and privacy risk committee oversees the various elements of cyber security and data privacy risks.

Risk controls and responses

For risks where our risk appetite is low, we take a robust approach to determine appropriate risk controls and responses. For these risks (typically regulatory and compliance risks) we have established policies and blueprints to guide the business in managing the risks. These risks are monitored formally by one or more of our various governance bodies, such as our Group risk and compliance committee, as well as by the Audit Committee. For other risks, which are typically strategic, pervasive or dynamic in nature, the risk controls and responses are determined on a case-by-case basis in line with the strategic goals of the organisation. Our approach to risk appetite provides the framework to consistently respond to risk and establish boundaries for coherent risk decision making. This element of the risk management framework has been enhanced during the current year to align the approach and adopt consistently. We will continue to improve and strengthen our risk appetite approach on a continuous improvement basis.

Governance, reporting and monitoring

A strong risk culture is at the heart of our RMF with clear risk ownership and proactive leadership. The responsibility for identifying, assessing, escalating and managing risks resides with management at a functional, business unit and executive level. The Board has overall responsibility for risk management and is actively engaged in risk discussions. The Audit Committee, on behalf of the Board, undertakes an annual effectiveness assessment of the RMF, with regular focus on specific emerging risks and a review across all principal risks, twice a year, which also supports the external reporting process, see **page 87**. The Group risk and compliance committee is responsible for the oversight of key risks on behalf of the Executive Committee. A new Chief Audit and Risk Officer (CARO) was appointed in April 2023.

Audit and assurance

Group Audit undertakes assurance activities including regular risk-based internal audits driven by the annual internal audit plan which is reviewed and approved by the Audit Committee. The internal audit plan is aligned to principal risks and remains under review and subject to change to reflect any updates to the risk profile through the year. The Audit Committee reviews and approves all changes to the audit plan and receives regular updates on the outcome of the work performed. Furthermore, second-line functions, such as: finance controls; ethics and compliance; and safety, systematically test key processes and controls established by management to mitigate risks. The work of second-line functions is subject to review by internal audit on a cyclical basis.

Principal risks and uncertainties

The most significant risks – those that could affect our strategic ambitions, future performance, viability and/or reputation – form our principal risks.

Our principal risks are detailed in the following pages. This includes a summary of key information, including the type of risk, links to our strategic drivers, risk movement, key responses and controls and the oversight committees at the Executive Committee and Board level. Please note, this list does not include all our risks. Additional risks, not presently known, or those we currently consider to be less material, may also have adverse effects. We also highlight principal risks that are included in our long-term viability scenarios, see **pages 46 and 47**.

At present, there continues to be a heightened level of geopolitical uncertainty due to wars and civic unrest, terrorism, elections and government restrictions. We have accordingly expanded the principal risk of pandemics into a wider risk definition of geopolitics and other global events, which includes the risk of future pandemics. Our approach to these events is to continue to scan the external environment for threats, assess the risk to our business and build resilience to minimise business disruption and prioritise the safety of our colleagues and customers in the event of such incidents. We understand the short-term risks and impacts and we have the right teams, governance mechanisms, customer offerings and strategies in place. However, the long-term impacts remain uncertain, and we will continue to monitor the geopolitical landscape closely and respond accordingly.

Our principal risks are interdependent and interconnected with each other, with comprehensive and cogent strategies designed to mitigate the cascading effects on our overall risk exposure.



Did you know:

We use a consistent assessment criterion to identify and prioritise risks at the Group, business unit and functional level, along with horizon scanning for emerging risk themes.

Figure 4

Lloyds Banking Group 2023 ARA, pp. 44, 144 – Emerging risk identification and details of horizon scanning

Emerging and horizon risks

The Group continues to focus on horizon scanning activity to inform and support identification of the most pertinent internal and external trends and developments.

Evolution of the Group's methodology for assessing and prioritising emerging risks

A series of deep dives on the 2022 emerging risk themes have taken place during the year. In addition, individual emerging risks themes have been taken to key executive-level committees throughout 2023, including the Board Risk Committee, with actions assigned to monitor more closely their future manifestation and potential opportunities.

The emerging risk themes were also considered as part of the annual financial planning cycle. Geopolitical risks, and how these may generate second order impacts for the Group, have been a focus.

Many emerging and horizon risk topics are reviewed on a recurring basis, alongside ongoing activity addressing their impacts. However, it is acknowledged that the nature of the emerging risks will evolve and could drive future trends in the long term which the Group will need to prepare for.

The 2023 emerging risk landscape has been simplified, combining emerging and strategic risks into a single view (see below), enabling greater management concentration on developing the appropriate responses. The Group will continue to monitor emerging and horizon risks, exploring how they may impact its future strategy, and how it can continue to best protect its customers, colleagues and shareholders.

For further information on the Board Risk Committee's Chair Report, see **pages 101 to 106**.

For further information on how the Group is managing key emerging risks through its strategy, see **page 144**.

Emerging risks

Customer propositions and societal expectations

The potential impacts of a failure to adapt our propositions to the continually evolving expectations and demographic of consumers, the evolution of and expectations relating to cybercrime, the threats posed by technology-enabled players and the risk of market disintermediation.

Environmental, social and governance expectations

Investor, shareholder and public perception of the Group's i) awareness of the ecological and environmental impacts associated with its operations and investments, ii) ability to offer sustainable financing options and services at pace, against a continuously evolving environmental and regulatory backdrop, and iii) role in supporting the UK to transition to a low carbon economy.

Global macroeconomic and geopolitical environment

Inability to navigate changing international regulations, including sanction and trade compliance, economic fragmentation, deglobalisation, and geopolitical events that may impact operations, customers and suppliers.

Strategic workforce vision

Failure to evolve the structure and skill set of a dynamic workforce in line with the Group's strategy, whilst maintaining pace with the industry and delivering strong customer outcomes.

Digital currencies and tokenisation

Failure to keep pace with the potential expansion of decentralised financial systems, launch of private sector or government-backed digital currencies, growth of blockchain technologies and asset tokenisation and adoption of technologies which support the mainstream utilisation of blockchain technologies.

Generative AI and ethical data practices

Failure to keep pace with technological advancements relating to Generative AI and machine learning whilst balancing the competing requirements to i) maximise customer opportunities through adoption, ii) maintain trust and confidence in customer data privacy, iii) protect our customers from fraud and economic crime, iv) ensure transparency on data ethics practices, v) adhere to evolving data protection regulations and vi) prepare for potential business model disruptions caused by adoption of the technology.

Operational elasticity

Failure to adequately prepare for the aggregate threat posed by cyber-attacks, disruption of service, third- or fourth-party supplier failure, technology outages or severe data loss.

UK political and macroeconomic environment

Failure to anticipate the longer-term impacts of a weak UK economy, quantitative tightening, change in government and the resulting policy and regulatory shifts (a bank levy, for example) and the potential consequences of the UK becoming less attractive to external investors.

Emerging risks

Background and framework

Understanding emerging risks is an essential component of the Group's risk management approach. It enables the Group to identify the most pertinent risks and opportunities, and to proactively respond through strategic planning and appropriate risk mitigation.

Whilst emerging risk is not a principal risk, if left undetected emerging risks have the potential to adversely impact the Group or result in missed opportunities.

Impacts from emerging risks on the Group's principal risks can materialise in two ways:

- Emerging risks can impact the Group's principal risks directly in the absence of an appropriate strategic response
- Emerging risks can be a source of new risks, dependent on our chosen response and the underlying assumptions on how given emerging risks may manifest

Where an emerging risk is considered material enough in its own right, the Group may choose to recognise the risk as a principal risk, with a recent example being climate risk. Such elevations are considered and approved through the Board Risk Committee as part of the annual refresh of the enterprise risk management framework.

Risk identification

The basis for risk identification is underpinned by our horizon scanning approach, supported by collaboration between functions across the Group. The Group works closely with regulatory authorities and industry bodies to ensure that the Group can monitor external developments and identify and respond to the evolving landscape, particularly in relation to regulatory and legal risk. In addition, the Group engages with external experts to gain external insight and context. This activity complements and builds upon the annual strategic planning cycle and is used to identify key external trends, risks and opportunities for the Group.

The Group continues to evolve its approach for the identification and prioritisation of emerging risks. During 2023, the Group continued to evolve its emerging risk methodology, refining and enhancing the process, placing greater focus on existing controls, to reflect the Group's position in its strategic transformation journey and the level of planned investment outlined in the Group's business plans.

The emerging risk methodology is centred around several key factors:

- The threat presented by a risk
- The Group's specific vulnerability to the risk
- The preparation and protection the Group has in place to manage or mitigate impacts
- The existing control environment and planned investment (new for 2023)

Our evolved approach has further streamlined the list of emerging risk themes from 10 to eight, enabling greater management concentration on developing the appropriate responses.

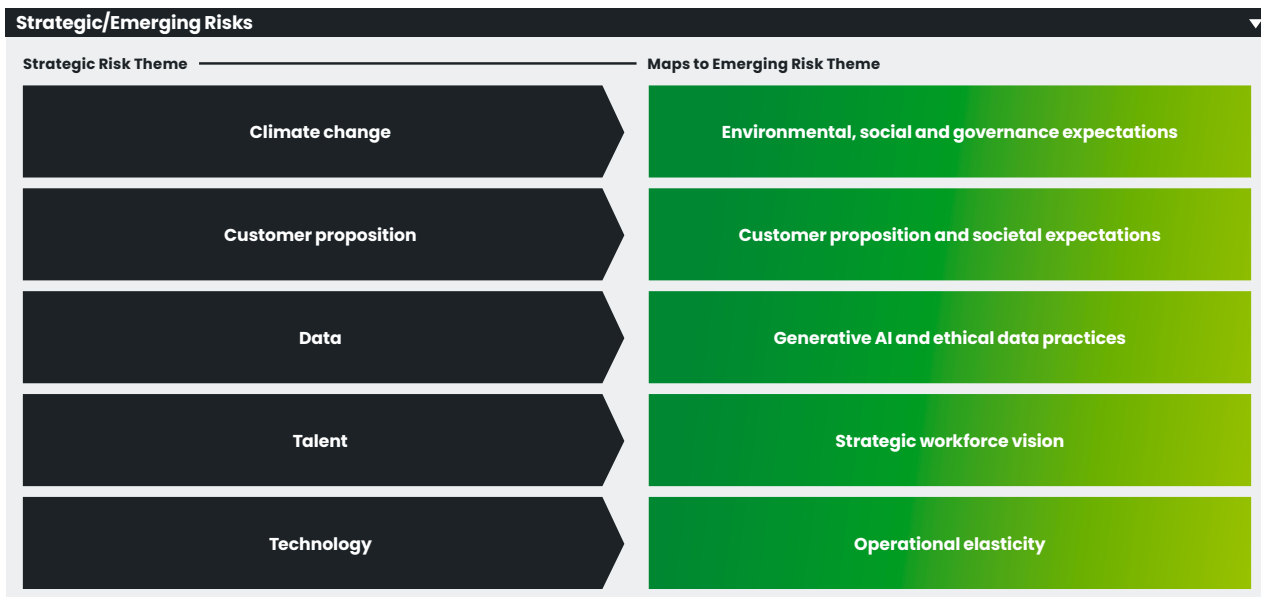
The emerging risk themes detailed in the risk overview section on **page 44**, align to the current primary risks the Group is managing and many of which (for example, operational elasticity and political and macroeconomic environment) are continuous areas of focus. The nature of emerging risks is expected to evolve and may require different ways to mitigate from the measures used today. The risks also correlate, for example customer propositions and societal expectations will be influenced by the UK political and macroeconomic environment.

Risk mitigation and monitoring

Emerging risks are currently managed through the Group's strategic risk framework, detailed on **page 196**.

Emerging risk themes have been discussed at executive-level committees throughout 2023, with key actions assigned to closely monitor their manifestation and potential opportunities, and in some cases, also forming part of the business planning process. Deep dives on selected emerging risk themes are also planned for 2024.

As part of the 2023 analysis, it has been identified that there is significant overlap with the previous strategic risk themes (climate change, customer proposition, organisational purpose, talent attraction and retention, and technology advances) and the emerging risk themes. This further supports our recommendation to merge these into a combined category of horizon and emerging risks from 2024 onwards. The graphic below indicates the mapping of the strategic risk themes to the emerging risk themes.



Source: <https://www.lloydsbankinggroup.com/assets/pdfs/investors/financial-performance/lloyds-banking-group-plc/2023/q4/2023-lbg-annual-report.pdf>

Figure 5

Croda 2023 ARA, p. 52 – Risk framework with clear delegation of responsibilities from the board to its committees

Our risk framework

What we monitor

Executive Risk Register

Summary of the principal risks facing us prepared by combining risks identified through the local bottom-up registers with top-down risks identified and owned by the Executive Committee.

Our risk landscape

Current risks

Risks we are managing now that could stop us achieving our strategic objectives.

Emerging risks

Risks with a future impact from external or internal opportunities or threats. These can be slow moving as well as rapid velocity.

What we assess

- **Risk ownership:** each risk has a named owner
- **Likelihood and impact:** globally applied 6x6 scoring scale
- **Gross risk:** before mitigating controls
- **Mitigating controls:** subject to internal audit review and monitoring
- **Net risk:** after mitigating controls are applied
- **Risk appetite:** defined at risk subcategory level
- **Actions:** identify further mitigation if required

Risk categories we assess

Six categories, 17 subcategories, over 60 generic risks, one framework:

- Strategic
- People and culture
- Process
- External environment
- Business systems and security
- Financial

Our bottom-up registers

The core of our risk assessment. Owned by market sectors, regions, manufacturing sites and functions, they identify local risks and mitigating controls arising from day-to-day operations globally.

How we monitor

Board

- Responsible for the risk framework and definition of risk appetite
- Reviews key risks with an opportunity for in-depth discussion of specific key risks and mitigating controls annually
- Approves the viability statement

Audit Committee

- Reviews the effectiveness of the Group risk management process
- Reviews assurance over mitigating controls, directing internal audit to undertake assurance reviews for selected key risks
- Reviews viability scenario assessments

Risk Committee

Chaired by Chief Financial Officer

- Meets quarterly to monitor and review risks (other than SHEQ, ethics and sustainability, which are delegated to other committees)
- Standing agenda items to monitor emerging risks, IT systems and cyber risks
- Receives an in-depth presentation of specific key risks and mitigating controls from risk owners
- Considers the results of internal audit work

Sustainability Committee

Chaired by Chief Sustainability Officer

- Meets quarterly to oversee the development, measurement and delivery of our sustainability strategy and the significance of climate related risks and opportunities
- Monitors against stretching targets and agreed KPIs

SHEQ Steering Committee

Chaired by President of Operations

- Meets quarterly to review SHEQ risks
- Monitors against stretching targets and agreed KPIs
- Considers the results of assurance audits over SHEQ controls

Ethics Committee

Chaired by Group General Counsel

- Meets quarterly to review ethics and compliance risks
- Monitors against agreed KPIs
- Considers the results of assurance audits over ethics controls

Source: <https://www.croda.com/mediaassets/files/corporate/2023-results/croda-annual-report-2023.pdf?la=en-GB>

Figure 6

SThree 2023 ARA, p. 76 – What risk attributes are monitored and assessed

What we review when assessing our principal and key risks:

Risk ownership: each risk has a named owner. In addition, each principal risk is sponsored by a member of the ExCo, who drives progress.	Risk tolerance: in data format, showing the amount of deviation from the risk appetite. ▶ Key risk indicators: quantitative measures that provide early signals of a change in the risk.
Likelihood and impact: globally applied five-by-five scoring matrix.	Actions: key controls in place and activities required for further mitigation if required.
Gross risk: before mitigating controls.	Impact on the Group's strategic pillars and interdependencies between principal risks.
Net risk: after mitigating controls are applied.	
Risk appetite: defined at principal risk level and categorised into five levels.	Any relevant emerging risks where the principal risk is impacted by or could impact the emerging risk.

All principal risks are detailed in a standardised statement. This ensures effective review, understanding and monitoring throughout the Group, together with consistency, both in terminology and the underlying assessment itself. As part of the top-down process, an updated assessment was completed for each principal risk by the relevant risk owner, working with the Executive Committee risk sponsor and the risk function. The statements are challenged and reviewed in detail by the Group Risk Committee, ExCo and by the Board twice a year. In addition, deep dive reviews are conducted by the Group Risk Committee throughout the year, the output of which is reviewed by the Audit & Risk Committee.

Figure 7

Reckitt 2023 ARA, 94 – Internal control responsibilities by line

achieving targeted goals is detailed in the Strategic Report, which can be found on pages 55 to 60.

The Viability Statement can be found on page 61.

The Statement of Directors' Responsibilities on page 137 details the Directors' responsibility for the Financial Statements, for disclosing relevant audit information to the External Auditor and for ensuring that the Annual Report is fair, balanced and understandable.

Internal controls framework

Internal control processes are implemented through clearly defined roles and responsibilities, supported by clear policies and procedures, delegated to the GEC and senior management. Reckitt operates a 'three lines of defence' model in monitoring internal control systems and managing risk.

1. Management in the first line ensures that controls, policies and procedures are followed in dealing with risks in day-to-day activities. Such risks are mitigated at source with controls embedded into relevant systems and processes. Supervisory controls, either at management level or through delegation, ensure appropriate checks and verifications take place, with any failures dealt with promptly. Throughout Reckitt, a key responsibility for any line manager is to ensure the achievement of business objectives with appropriate risk management and internal control systems.

2. Each function and GBU has its own management which acts as a second line of oversight. This second line sets the local level policies and procedures, specific to its own business environment, subject to Group policy and authorisation. The second line further acts in an oversight capacity over the implementation of controls in the first line.

The financial performance of each function and GBU is monitored against pre-approved budgets and forecasts ultimately overseen by the executive management and the Board.

As part of the second line, the corporate control team identifies financial risks and mitigates these with appropriate internal controls, set out through minimum expected financial control requirements. The effectiveness of the global financial control framework is reviewed annually. Further, the Group's compliance controls include the operation of an independent and anonymous 'Speak Up' whistle-blowing hotline, annual management reviews and the provision of training specific to individual needs within the business.

3. The third line of defence is provided by the internal audit function which provides independent and objective assurance to management and the Committee on the adequacy and effectiveness of risk management systems and internal controls operated by the first and second lines of defence. Internal audit also facilitates the risk management process.

Reckitt's internal control framework provides 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 are understood and managed.

The corporate control team is accountable for managing global financial control policies and frameworks and for monitoring the effectiveness of the Group's internal financial control environment. Corporate control is responsible for reporting and monitoring controls at local, GBU

and global levels, working with markets to improve risk and controls capability and to support the development of remediation plans and corrective actions for financial control weaknesses.

To improve the maturity of the control environment and meet upcoming changes to the Code, the Company has established a multi-year controls transformation programme. In 2023, the controls transformation programme launched an updated, standardised and risk-focused controls framework for financial and IT general controls, including new evidence standards to enable consistent documentation of the operating effectiveness of financial and IT general controls. Following launch, the second line of defence team, supported by external advisors, conducted a comprehensive fit-gap assessment to determine the required uplift to comply with the new framework and evidence standards. As anticipated, gaps versus the framework and standard have been identified in relation to the retention of evidence and the formality and consistency of control operation. Where required, plans have been developed and remediation activity is underway in markets, IT and group. In 2023, the effectiveness of the global financial control framework has been assessed through analysis of the results from the fit-gap assessment and subsequent remediation, alongside consideration of findings on the internal control environment from internal audits conducted in 2023.

At each meeting, the Committee reviews a report outlining the status of the controls transformation programme, the results of the fit-gap assessment and remediation progress, and other notable controls activity since the previous meeting. In 2024, assurance over

Figure 8

The Weir Group 2023 ARA, p. 90 – Four tiers of internal control

Risk management and internal controls

In accordance with the UK Corporate Governance Code and the accompanying FRC's Guidance on Risk Management and Internal Controls, the Group has an ongoing process for identifying, evaluating and managing the significant risks through a comprehensive internal control framework. This four-tier process has been in place throughout 2023 and is described in more detail below.

The Board, in seeking to achieve the Group's business objectives, cannot offer an absolute guarantee that the application of a risk management process will overcome, eliminate or mitigate all significant risks. However, by further developing and operating an annual and ongoing risk management process to identify, report and manage significant risks, the Board seeks to provide a reasonable assurance against material misstatement or loss. More information on how the Group seeks to manage risk can be found on pages 60 to 69.

The Audit Committee conducted a review of the effectiveness of the Group's systems of internal control and risk management during 2023 on behalf of the Board, as set out on page 99. The Group's internal control procedures described on page 101 of the Audit Committee Report do not cover joint venture interests. We have Board representation on each of our joint venture companies, where separate, albeit similar, internal control frameworks have been adopted.

Tier 1: Functional and front line controls

This includes a wide spectrum of controls common to many organisations, including: standard operating procedures and policies; a comprehensive financial planning and reporting system, including quarterly forecasting; regular performance appraisals and training for employees; restricted access to financial systems and data; delegated authority matrices for the review and approval of key transactions, arrangements and other corporate actions; protective clothing and equipment to protect our people from harm; IT and data and cyber security controls; business continuity planning; and assessment procedures for potential new recruits.

Tier 2: Monitoring and oversight controls

There is a clearly defined organisational structure within which roles and responsibilities are articulated. There are monitoring controls at operating company, regional, Divisional and Group level, including standard key performance indicators, with action plans drawn up, implemented and monitored to address any underperforming areas.

A Compliance Scorecard self-assessment is completed and reported by all operating companies twice per annum. The Scorecard assesses compliance with Group policies and procedures, see page 101 for further details.

Financial monitoring includes comparing actual results with the forecast and prior year position on a monthly and year-to-date basis. Significant variances are highlighted to Directors on a timely basis, allowing appropriate action to be taken.

Tier 3: Assurance activities

We obtain a wide range of both internal and external assurances to provide comfort to management and the Board that our controls are providing adequate protection from risk and are operating as we would expect.

These sources of assurance were reviewed by the Board during the year, and principally comprise external audit, internal audit, SHE audits and IT audits. As described in the Audit Committee Report on page 102 and in the Sustainability section of the strategic report on page 58, we are also enhancing our internal capabilities around assurance on ESG and non-financial reporting-related matters.

The various audit teams plan their activities on a risk basis, ensuring resources are directed at the areas of greatest need. Issues and recommendations to enhance controls are reported to management to ensure timely action can be taken, with oversight provided from the relevant governance committees, including the Audit Committee and the Excellence Committees.

Our internal control framework has four key tiers:



Tier 4: Ethical and cultural environment

We are committed to doing business at all times in an ethical and transparent manner. This is supported by the Weir values, which are the core behaviours we expect our people to live by in their working lives. The Weir Code of Conduct also contributes to our culture, providing a high benchmark by which we expect our business to be conducted. You can read more about our culture on page 81.

Any examples of unethical behaviour are dealt with appropriately and promptly. The Group has a combination of formal and informal channels to raise concerns regarding unethical behaviour, including the Weir Ethics Hotline, which enables any member of the workforce to raise concerns in confidence and, if they wish, anonymously. The Board reviews the operation of the Hotline on an annual basis, and is provided with updates regarding the Hotline routinely through the Corporate Services Report which is presented at every Board meeting. The Group's Compliance function works closely with the business to ensure that any matters raised via the Weir Ethics Hotline are investigated in a fair and impartial manner consistent with the Group Investigation Protocol, and the Board is notified of follow-up actions taken where appropriate to do so.

The Responsible Business Practices section on page 58 provides more details on the Group's activities to promote ethical behaviour and the Weir Ethics Hotline.

The Audit Committee, our internal audit function and our external auditors

Details of the roles and responsibilities of the Audit Committee and its members can be found in the Audit Committee Report on pages 98 to 108. Information on the role of the Group's internal audit function, as well as that of the Company's external auditors, is also contained within the Audit Committee Report.

Source: <https://www.global.weir/siteassets/pdfs/2023-annual-report/weir-group-2023-annual-report.pdf>

Figure 9

BAE Systems 2023 ARA, p. 87 – Operational framework listing out key policies

Operational Framework

Agreed annually by the Board, the Operational Framework is a comprehensive statement of mandated governance requirements and delegated responsibilities. The UK Corporate Governance Code's (the Code) principles are embedded within the Operational Framework, and its policies and processes underpin all the disclosures made by the Board pursuant to the Code's provisions.

Our Operational Framework provides a stable foundation from which to deliver our strategy, improve our Group performance and continue to develop our culture.

It is mandatory across all wholly-owned entities and details our organisation, governance framework, core business practices and delegated authorities.

Internal controls

Core Business Processes

This describes the reporting and reviews mandated by the Operational Framework, which provide upwards visibility of project and business performance.

Operational Assurance

A process through which line and functional leaders respectively confirm twice yearly that their businesses and functions are compliant with the Operational Framework.

Internal Audit

Assesses the effectiveness of internal controls through a programme of reviews based on a continuous assessment of business risk across the Group.

We take pride in managing our operations effectively and responsibly

Responsible trading principles

How we conduct business is fundamental to the success of our Company and we mandate a principles-based approach to our business activity. We do not compromise on the way we conduct business, and consistency of this approach is key in defining our reputation.

Product safety policy

We set out principles which describe our approach to product safety to reduce the risk of unintentional harm to people, property and the environment. They apply throughout the life of the Product and throughout the supply chain.

Workplace and operational environment

Our people management expectations are communicated to all employees and set out within our People Policy. We have a zero tolerance policy regarding corruption and our employees are made aware of their role in ensuring we maintain high standards of ethical conduct. Pages 62 to 64 provide further detail about our anti-corruption programme.

The safety and wellbeing of our employees is paramount and our high standards for Health and Safety management provide a common framework to guide our workforce and further information can be found on page 58.

We use our expertise to reduce our global environmental impacts and to develop products and services for our customers which reduce their impacts on the environment. Our climate transition strategy and impact on the environment including greenhouse gas (GHG) emissions, efficient use of resources, land use and biodiversity, and the environmental impact of the Group's supply chain is overseen by the Environmental, Social and Governance Committee.

We are committed to ensuring that IT systems and services are used in a manner which promotes effective communication and working practices within the organisation and to preventing damage to its business or reputation through misuse of those systems.

With the support of our Internal Audit team, our IT assurance and governance programme has been developed to support the effective management of cyber risks.

Suppliers

The Group depends upon its suppliers to provide fully compliant, cost-effective equipment, goods, services and solutions, which are an integral part of the world-class products required by our customers, and also support the effective operations of our businesses and the Group's standards of business conduct. Our supply chain management and Supplier Principles – Guidance for Responsible Business (the Supplier Principles) are focused on high achievement of our standards. Our supplier contracts contain anti-corruption and anti-bribery provisions and stipulate the expectation to compliance, meet our standards on ethical business conduct and Supplier Principles, including safety, environment and human rights.

Product trading policy

Underpins all of our business activity and the policy applies to all Company products, trading, and throughout the product lifecycle. The policy is used to reflect the Company's standards of integrity and help us to thoroughly evaluate the opportunities we pursue.

Risk management policy

We set clear requirements for the management and reporting of risks in support of the delivery of our strategy. Project risks are managed through our Lifecycle Management Framework.

Core business processes

Our IBP represents a common process with standard outputs and requirements that produces an integrated strategic business plan for the Group and also for each of its businesses over the following five years. The IBP is reviewed each year by the Board as part of its strategy review process. Once approved, the IBP provides the basis for setting all detailed financial budgets and strategic actions across the businesses, and is subsequently used by the Board to monitor performance.

As mandated by the Operational Framework, Businesses and Group functions complete a bi-annual Operational Assurance Statement (OAS). The OAS is in two parts: a self-assessment of compliance with the Operational Framework; and a report showing the key financial and non-financial risks for the relevant business

and Group functions. Together with reviews undertaken by Internal Audit and the work of the external auditors, the OAS forms the Group's process for reviewing the effectiveness of the system of internal controls.

Lifecycle Management (LCM) Framework describes our approach to the assurance of Projects. LCM is integral to the successful execution of the Group's projects and programmes. Its application provides progressive risk-based assurance throughout the lifecycle to aid decisions, supporting delivery of projects to achieve customer satisfaction, schedule and financial requirements.

The purpose of the Mergers, Acquisitions and Disposals process is to provide a structured approach to managing the acquisitions, strategic joint ventures and disposals. It forms a part of our Strategy and Planning framework in order to support the delivery of the IBP.

National security arrangements

The Group is subject to various national security requirements which are an important part of how we operate as a defence company and meet the needs of our customers. Due to the nature of its activities, the UK government holds a Special Share in the Company, ensuring that the Company cannot be non-British controlled. We also have a Special Security Agreement with the US Department of Defense addressing national security matters relating to the ownership and control of our US defence businesses. Through the Special Security Agreement, our governance structure is augmented by the BAE Systems, Inc. board, which is populated by experienced individuals drawn principally from the US armed forces and intelligence community, and also former Members of Congress.

Similarly, our Australian operations are subject to an Overarching Deed with the Commonwealth of Australia which protects national security and other interests, and allows the Group to own and manage certain Australian defence-related industrial assets. These national security arrangements are an important part of our governance.

Source: https://investors.baesystems.com/~/_media/Files/B/BAE-Systems-Investor/investors/annual-reports/2023-annual-report.pdf

Figure 10

3i Group 2024 ARA, p. 127 – Key control framework

<p>Investment process</p> <ul style="list-style-type: none"> ▶ Due diligence process ▶ Investment procedures ▶ Investment Committee review and approval ▶ ESG assessment ▶ Responsible Investment policy 	<p>Investment portfolio companies</p> <ul style="list-style-type: none"> ▶ 3i Group board representatives ▶ Active management of senior appointments ▶ Minimum ESG requirements 	<p>Investment portfolio management</p> <ul style="list-style-type: none"> ▶ Procedures for portfolio management ▶ Monthly portfolio company dashboards and performance monitoring ▶ Six-monthly investment and portfolio company reviews, including reporting against ESG requirements
<p>Viability and going concern</p> <ul style="list-style-type: none"> ▶ Stress testing methodology and modelling ▶ Analysis of assets and liabilities ▶ Capital adequacy review process ▶ Group strategy and liquidity forecasting models 	<p>Valuation process</p> <ul style="list-style-type: none"> ▶ Approved Valuations policy ▶ Investment and portfolio company review processes ▶ Central oversight by the Valuations team, Investment Committee and Valuations Committee 	<p>Financial reporting</p> <ul style="list-style-type: none"> ▶ Framework of key financial controls and reconciliations ▶ Portfolio, fund and partnership accounting processes ▶ Documented analyses of complex transactions and changes in accounting requirements and disclosures ▶ Operating expense budget
<p>People and culture</p> <ul style="list-style-type: none"> ▶ Values framework and HR policies ▶ Performance management framework ▶ Remuneration policies ▶ Conduct and compliance policies and monitoring ▶ Succession planning process 	<p>Advisory relationships</p> <ul style="list-style-type: none"> ▶ Pre-approved suppliers of investment due diligence services ▶ Tendering and approval process for other advisers, eg legal, tax ▶ Monitoring of performance and patronage ▶ Confidentiality and conflicts management 	<p>Third-party service suppliers</p> <ul style="list-style-type: none"> ▶ Use of 3i Group's Supplier Relationship Management tool ▶ Required contractual protections, eg data security and business continuity ▶ Oversight and governance frameworks for critical suppliers ▶ Independent service organisation reports
<p>Balance sheet management</p> <ul style="list-style-type: none"> ▶ Treasury policy and control framework ▶ Liquidity monitoring framework ▶ Fund transfer and release controls ▶ Portfolio concentration and vintage control monitoring framework ▶ FX hedging programmes 	<p>Change management</p> <ul style="list-style-type: none"> ▶ Approval process for changes to corporate structure or new products/ business areas ▶ Ongoing monitoring of legal and regulatory changes ▶ Active participation and engagement with government, regulators and trade bodies ▶ Business systems project governance and oversight 	<p>IT systems and security</p> <ul style="list-style-type: none"> ▶ IT governance and policy framework ▶ Access and data security controls ▶ Back-up and disaster recovery procedures and testing ▶ IT and cyber security monitoring and control framework, and regular penetration tests ▶ Staff cyber security awareness training

Figure 11

Derwent London 2023 ARA, p. 149 – Detail of internal financial controls

Internal audit

The Internal Audit Plan for 2023 was jointly approved by the Risk and Audit Committees and was comprised of risk-based reviews across a range of business areas. Both Committees receive reports on internal audit activity and monitor the status of internal audit recommendations.

During 2023, a formal review of the effectiveness of the internal auditor and the internal audit process was conducted. It was concluded that the process had been conducted effectively and that the independent assurance received through internal audits had been beneficial to the Committee and management. Audits performed during 2023:

- Intelligent buildings implementation and management
- Energy Performance Certificate (EPC) compliance
- Supplier selection and due diligence
- Fraud controls
- IT development controls
- Financial controls

Annual review of the internal audit function

The internal audit function has been outsourced to RSM since December 2018, and they have carried out all reviews during 2023. In line with the Group's commitment to continuously enhance the internal control environment, the Audit and Risk Committees reviewed the model for the provision of internal audit services and decided to bring the function in-house.

Julie Schutz, our new Head of Internal Audit, is a Chartered Accountant with extensive experience in the provision of risk and assurance services across a diverse range of industries. Julie will work closely with the Risk and Audit Committees to develop and deliver a risk-based internal audit programme for 2024. The plan will include a combination of both assurance activities over key risk areas and advisory work, which will support the business in further strengthening its control environment.



Internal audit is responsible for fostering a culture of accountability and continuous improvement.

Julie Schutz
Head of Internal Audit

Internal controls

Our internal financial controls environment allows the Company to safeguard its assets, prevent and detect material fraud and errors, and ensure accuracy and completeness of its accounting records which are used to produce reliable financial information. During 2023, we have undertaken the following actions to further strengthen our financial controls:

- Cyber risk continues to be an area of key focus and is subject to independent testing ([pages 162 and 163](#)). The Digital Innovation & Technology (DIT) team enhanced our Business Continuity Plan and conducted a full disaster recovery test with minor lessons learned to further resilience.
- Implementation of a new continuous learning approach to cyber awareness. Staff are now completing 'small' modules throughout the year enabling us to raise awareness of new attack methods in real-time and targeting those at heightened risk due to their role type.
- Ongoing documentation, review and enhancement of key financial processes and controls as part of the Internal Controls Project.
- Implementation of a new HR solution to automate workflows and introduce more preventative controls. The payroll module is to go live during 2024.
- Development of a new supplier set-up portal to strengthen controls by automating due diligence checks.

Effectiveness review

The Committee receives detailed reports on the operation and effectiveness of the internal financial controls from members of the senior management team and our internal auditors. In addition, the outcome of the external audit at year end and the half year review are considered in respect of ongoing enhancements to internal controls.

On an annual basis, the Committee reviews the Group's fraud risk management framework, of which a fraud risk assessment is a key component. The framework helps management assess and improve upon its fraud resilience measures across a range of key components, while the risk assessment sets out the detailed controls which safeguard the Company's assets and help prevent and detect fraud and errors. A heat map summarises residual risk scores based on the fraud risk assessment, and those risks with scores above tolerance levels have action plans in place to help further mitigate the residual risk.

As training and staff awareness forms part of the Group's internal control framework, the Risk Committee receives updates on key policies and procedures in place and how these are being communicated to, and complied with, by our staff. Further information is on [pages 159 and 165](#).

Following the Audit and Risk Committees' reviews (see [page 92](#)), the Chairs of each Committee confirmed to the Board that they are satisfied that the Group's internal control framework (financial and non-financial) and risk management procedures:

- operated effectively throughout the period; and
- are in accordance with the guidance contained within the FRC's Guidance on Risk Management, Internal Control and Related Financial and Business Reporting.

Internal financial controls

Our internal financial controls operate within the following control environment and context:

- **Company culture:** We have a defined set of values and strategic objectives that are supported by a Code of Conduct and Business Ethics which creates an environment that values integrity, openness, transparency and building long-term relationships. Our culture promotes collaboration and encourages employees to ask questions and challenge decisions.
- **Workforce:** Our flat structure and modest headcount (relative to asset values) allows for the close supervision and monitoring of activity by members of the Executive Committee.
- **Group structure:** Relatively simple and transparent Group legal structure with relatively few subsidiaries and joint ventures.
- **Income/costs:** Rent, service charge, administrative costs (mainly salaries), interest and other finance costs are predictable. Quarterly management accounts are prepared that analyse income and expenditure and compare them with the prior year and budget, with unexpected variances investigated and explained.
- **Capital costs:** The largest costs incurred relate to capital expenditure. All capex on investment properties is approved and, where material, is subject to external confirmation, before being paid. These approved budgets are monitored internally.

Overview of internal financial controls:

Governance framework	Our governance framework (see page 127) supports effective internal control through an approved schedule of matters reserved for decision by the Board and the Executive Directors, supported by defined responsibilities, levels of delegated authority and supporting committees.
Risk identification and monitoring	Management regularly review and assess key risks facing the Group, including scenarios which could result in material financial and/or tax fraud or errors. Key risks are documented in risk registers, along with a schedule of key controls and key risk indicators. The schedule of key controls provides evidence of how the controls are being operated, their effectiveness and areas of potential weakness and further improvement. Risk management activities are overseen by the Risk Committee, and their report is on pages 156 to 165 .
Financial controls	Comprehensive systems of financial control are in place including an annual budgeting exercise with three rolling forecasts, as well as a five-year strategic review. Breakeven and sensitivity analyses are included in both the five-year review and the rolling forecasts, with quarterly variance analysis performed between budget and actuals. A range of both preventative and detective controls, including segregation of duties, reconciliations, approvals, management reviews and exception reporting helps ensure accuracy and completeness of financial records.
Treasury and tax controls	Treasury activities are controlled by the Chief Financial Officer and Group Financial Controller. All large and/or complex transactions are discussed in advance with the Board and Executive Directors, executed in line with delegated authority levels and externally reviewed by our advisers. Taxation is a complex area and is subject to frequent external review. Corporate tax returns are prepared by the Tax Analyst, reviewed and prepared internally by senior members of the tax department and externally by RSM on a sample basis. Other higher risk areas like VAT, PAYE and CIS are subject to thorough examination and testing. We maintain an open relationship with HMRC who assessed our tax status in 2023 as 'low risk' in all categories. Further information on tax governance is on page 58 .
IT controls	IT general controls are a fundamental part of the financial control environment and apply to applications, databases and operating systems. They ensure appropriate access to, and integrity of our data, which ultimately flows through to the financial statements. A robust system of back up is in place to protect against the potential loss or corruption of data against the backdrop of ever-evolving cyber threats.
Training and staff awareness	Key policies and procedures are available to employees on our Group intranet. Employees are required to confirm their understanding of our key internal policies upon joining, and periodically thereafter as required for compliance purposes. Cyber risk training is delivered throughout the year to help maintain high levels of staff awareness and core system training is delivered when new systems are implemented, or ways of working are changed. The Group operates a 'Speak Up' Policy which includes access to an anonymous reporting hotline to raise any concerns of misconduct, wrongdoing, or fraud (see page 128).
External evaluation	The outsourced internal auditors, RSM, performed various assurance reviews over key financial controls as part of the 2023 Internal Audit Plan. The implementation of recommendations arising from the reviews are monitored by the Risk and Audit Committees. During the year, it was decided that the provision of internal audit services would be brought in-house (see page 148). The Group's VAT procedures are subject to ongoing periodic review by external advisers. An independent review of particular financial controls is undertaken with assistance from external advisers, as required. An annual credit rating review is performed by an external agency and each year, at renewal, a comprehensive review of the Group's insurance cover is prepared by our independent insurance adviser.

Source: <https://www.derwentlondon.com/uploads/downloads/RA-2023-Final-WEB-INTERACTIVE.pdf>

Figure 12

Intertek Group 2023 ARA, p. 76 – Control self-assessment process in place

Internal control and risk management systems

(...)

In order to provide assurance that the Intertek Group 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 with 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 Group 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 2024.

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 Group's operational and financial structure, and in order to enhance the alignment of the self-assessment to the assurance process.

Figure 13

Serco Group 2023 ARA, p. 33 – Second line controls testing

Risk management process

(...)

As part of our ERM approach we have dedicated Compliance Assurance teams which operate as a second line function focusing on validation and testing of key controls to augment annual control self-assessments and biannual compliance assurance attestation statements. Key controls mapped against our principal risks, significant local risks, our Serco Group Management System and testing plans are reviewed annually by the Group Compliance Assurance team to identify and respond to any significant amendments in the control environment. While many controls are tailored to meet Divisional requirements, there are consistent themes across our control environment to include; clear oversight and reporting by Divisional management teams; robust bid governance processes; a focus on the health, safety and well-being of our colleagues and service users and the prioritisation of maintaining integrity and a strong ethics culture. In addition to the work of our in-house Compliance Assurance teams, augmented by external partners in certain specialist areas, we are also subject to significant third line assurance activities and audits delivered through our in-house Internal Audit team, external third parties, certification standards and customer requirements in our varied service lines and business units. These external reviews include those that support the range of ISO certifications we manage across the business as well as independent performance and regulatory reports on Serco Group operations.

Figure 14

Beazley 2023 ARA, p. 117 – Internal audit involvement in internal controls assurance

Internal controls and systems

(...)

The Internal Audit function separately reports independently to the Audit Committee on the design and operating effectiveness of the system of internal controls covering the integrity of the Group's financial statements and reports, compliance with laws and regulations, corporate policies and the effective management of risks faced by the Group in executing its strategic and tactical operating plans. For more information see the Audit Committee report from page 106.

Illustrative examples for 3.4.1 Mitigating actions

Figure 15

Rolls Royce Holdings 2023 ARA, p. 52 – Assurance activities and providers against each principal risk

PRINCIPAL RISKS – PILLARS

Change in risk level: Increased Static Decreased

Safety

PRINCIPAL RISK DESCRIPTION

Product: Failure to provide safe products
People: Failure to create a place to work which minimises the risk of harm to our people, those who work with us, and the environment, would adversely affect our reputation and long-term sustainability

CONTROLS AND MITIGATING ACTIONS

- Product:**
- Our product safety management system includes controls designed to reduce our safety risks as far as is reasonably practicable and to meet or exceed relevant company, legal, regulatory and industry requirements
 - We verify and approve product design
 - We test adherence to quality standards during manufacturing
 - We validate conformance to specification for our own products and those of our suppliers
 - We mandate safety awareness training
 - We use engine health monitoring to provide early warning of product issues
 - We take out relevant and appropriate insurance
- People:**
- Our HSE management system includes activities and controls designed to reduce our safety risks as far as is reasonably practicable and to meet or exceed relevant company, legal, regulatory and industry requirements
 - We reinforce our journey to zero harm
 - We use our crisis management framework

ASSURANCE ACTIVITIES AND PROVIDERS	OVERSIGHT FORUM(S)	BUSINESS MODEL
<p>Product</p> <ul style="list-style-type: none"> – Product safety assurance team – Product safety board – Technical product lifecycle audits <p>People</p> <ul style="list-style-type: none"> – Safety case interventions – HSE audit team 	<ul style="list-style-type: none"> – Safety, Energy Transition & Tech Committee 	<ul style="list-style-type: none"> – Our role in society – Our business model drivers – Our uniqueness
<p>WHAT HAS CHANGED IN 2023?</p> <p>No overall change in risk status.</p> <p>As part of transformation, we are bringing together engineering technology and safety into one organisation, ET&S, with product safety at its heart (see page 9).</p> <p>People safety related metrics can be found on pages 44 to 45.</p>		

Source: https://www.rolls-royce.com/~/_media/Files/R/Rolls-Royce/documents/annual-report/2024/2023-annual-report.pdf

Figure 16

IHG 2023 ARA, p. 46 – Internal audit plan considerations against each principal risk

In pursuing our ambition, we face inherent uncertainties relating to:

Our ability to attract and retain talent and capability

Executive Risk Sponsor:
Chief Human Resources Officer

Link to strategy:



Why these uncertainties are important to the achievement of our strategic objectives over the next 2-3 years

Our growth ambitions are dependent on high-quality talent across our hotels, reservations offices and corporate functions. We continue to face a competitive market and uncertainties in relation to the availability, recruitment and retention of sufficient quality, quantity and diversity of talent, for example, next-generation hotel GMs to support our Luxury & Lifestyle growth and a robust pipeline of leadership succession talent.

Our priority to care for our people, communities and planet also means that we need to balance short- and longer-term growth risks and opportunities with our broader responsibilities and commitments. This requires us to enable colleague development and growth, to look out for our colleagues' wellbeing during the current cost of living crisis in many locations we operate within, and to maintain productivity, collaboration and appropriate labour relations. This also necessitates continued adaptation and innovation of our operational procedures and remuneration structures to be agile to the changing interests of our stakeholders.

IHG has the ability to manage talent and retention risks directly in relation to IHG employees but relies on owners and third-party suppliers to manage these risks within their businesses. Our Procurement, Legal and Risk teams also consider indirect workforce risks.

If we do not anticipate and respond appropriately to this uncertainty, it could impact our ability to operate and grow hotels, the effectiveness and efficiency of our key corporate functions and executive leadership, and it could heighten risks of exposure to non-compliance or litigation.

How senior management and the Board obtained assurance in our risk management and resilience in 2023

The Board considers reporting and insight from management, including on:

- overall HR and talent strategy;
- remuneration and incentive strategy and policy, including directors and executive management and wider structures for all colleagues, supported by external advisers;
- specific talent and succession planning;
- DE&I updates; and
- direct employee feedback via the Voice of the Employee programme.

The Executive Committee directly reviews talent (both as a group and through individual talent reviews with the CEO) and receives regular updates on colleague engagement and broader culture and behaviours. The HR team also has a dedicated Talent & Leadership steering committee. Regular all-employee calls are held with the Chief Executive Officer, and there are ongoing leadership communications and virtual team meetings at regional and functional levels.

The 2023 Internal Audit plan has provided independent assurance on employee relations management, recruitment of critical GM talent and implementation and data integrity checks within a strategic HR system transformation.

Data and information usage, storage, security and transfer

Executive Risk Sponsor:
Chief Commercial and Technology Officer, Chief Customer Officer and Executive Vice President General Counsel and Company Secretary

Link to strategy:



By its nature, our business involves the management of large volumes of data globally and our stakeholders (including guests, loyalty members, colleagues, owners and external authorities) expect that this will be done safely and responsibly.

Our strategic objectives continue to transform how we use our commercial and marketing data to improve and personalise the customer experience, grow loyalty and empower our owners to make better decisions. This involves a roadmap engaging many IHG teams in many initiatives, including increasing use of cloud-based applications, storage and partnering with third-party specialists, as well as exploiting technology advancements and innovation, involving the use of personal data and artificial intelligence. Our growth strategies, including new business partnerships, also increase the complexity of data flows.

The opportunities presented by this ambition are consciously balanced with the inherent exposures our digital footprint presents to data, information security and privacy-related threats, including threat actors (e.g. criminals, third parties and inherent colleague risk), and the need to demonstrate to stakeholders that we are using data appropriately. This includes an evolving global and local regulatory environment and requirements for localisation of data in certain territories. Our ability to deliver our strategies confidently is based on investments in recent years in cybersecurity and information governance and the maturing of our risk management system.

If we fail to respond to this risk effectively, we face operational, financial and reputational impacts to the range of high-value assets we are responsible for, or we may miss chances to capitalise on the opportunities that effective use of data can bring, including to our guests, owners and loyalty members. In addition, if the data we use is not accurate, this may impair decision-making and/or lead to lack of trust or satisfaction by our guests, loyalty members or owners.

The Board considers reporting and insight from management, including:

- governance over developments in cross-border data transfer arrangements to respond to evolving regulation;
- direct presentations from the Chief Information Security Officer, including third-party expertise on risk assessments, progress on the information security roadmap and advice on specific topics;
- within the wider roadmap, specific lessons learned and initiatives to further enhance security posture following the criminal unauthorised system access event in 2022 and to respond to the ongoing dynamic cybersecurity threat environment;
- information on emerging risks and opportunities of generative artificial intelligence, how management teams are considering these risks and how they relate to the broader assessment of principal risks;
- updates on the cyber insurance renewal strategy;
- second-line reporting on our privacy programme and policies for handling information responsibly; and
- updates on metric integrity, including review of ESG data principles and future assurance arrangements, supported by third-party experts.

The Executive Committee reviews specific areas of digital strategy, for example in relation to Greater China, and receives briefings from the Chief Information Security Officer on emerging risks during the year.

The Internal Audit plan includes independent focus on governance of both cybersecurity and data and information, assurance on foundational controls at both corporate and hotel levels and, for example, in relation to data transfers within our loyalty programme, third parties and cloud environments.

In pursuing our ambition, we face inherent uncertainties relating to:

Ethical and social expectations

Executive Risk Sponsor:
Executive Vice President
General Counsel
and Company Secretary,
Executive Vice President
Global Corporate Affairs
and Chief Human
Resources Officer

Link to strategy:



Why these uncertainties are important to the achievement of our strategic objectives over the next 2-3 years

As IHG operates in more than 100 countries and continues to explore new opportunities for growth, we are continually exposed to evolving expectations from our stakeholders in relation to ethical and responsible business conduct, extending beyond compliance with laws. We are committed to monitoring, reinforcing and communicating the continued effectiveness of our human rights approach, our social responsibility and environmental performance, and recognise that expectations are increasing for us to manage and drive ethical and responsible business through our supply chains and across our wider business, which involves extensive engagement with our franchisees around the world.

Our stated priority to care for our people, communities and planet creates risks and opportunities in relation to our growth ambitions, including how we build brands which guests and owners love while also considering our wider stakeholder responsibilities, including to our colleagues, guests, workers in our supply chains and our local communities in a challenging operating environment in many markets. We manage these risks carefully so as to operate responsibly and with integrity, and to guide decision-making across IHG's corporate and hotel operations.

If we fail to effectively respond to this risk, it has the potential to impact our performance and growth in key markets as well as cause reputational damage with respect to key stakeholder and investor expectations.

How senior management and the Board obtained assurance in our risk management and resilience in 2023

The Board considers reporting and insight from management, including:

- requests for Board approval of the Code of Conduct, the Supplier Code of Conduct, the Communities Policy and the Human Rights Policy;
- second-line reports on ethics and compliance strategy, including external benchmarking where appropriate (e.g. Transparency International UK's Corporate Anti-Corruption Benchmark);
- reports from Internal Audit on confidential reporting arrangements and updates from our Voice of the Employee programme;
- updates provided and awareness raising from the external Auditor on ESG and climate-related reporting and from external specialist advisers; and
- further second-line function reports on our communities, human rights and responsible procurement programmes and key disclosures including the Modern Slavery Statement.

The Executive Committee monitors our ambition and commitments to our people, communities and planet, including the progress of set initiatives and how these objectives interrelate to our growth strategy.

The Internal Audit plan includes independent focus on ethics and compliance, including consideration of management and external assessments of maturity, controls relating to marketing and commercial campaigns, due diligence controls and broader ESG-related programme governance.

Legal and regulatory complexity or litigation trends

Executive Risk Sponsor:
Executive Vice President
General Counsel
and Company Secretary

Link to strategy:



The global business regulatory and contractual environment continues to evolve rapidly, with ongoing legislative changes in many jurisdictions that will affect the way in which we operate our existing business and where we target growth or digital innovation. This includes the nature of our franchise relationships with hotel owners, our interactions with our suppliers, and our responsibilities to consumers and to colleagues. We consider such exposures carefully as part of our decision-making, drawing on an extensive network of legal advisers.

These changing laws and regulations continue to add complexity and uncertainty to compliance, particularly where there are diverging standards between territories (for example, in relation to increasing protections and conditions on cross-border data transfer). The ongoing use of sanctions and countermeasures as foreign policy tools also continues to present operational challenges and associated legal and regulatory exposures.

We recognise that failing to address this risk effectively, and non-compliance and/or inadequate compliance, could expose us to regulatory breaches, significant monetary and non-monetary penalties, adverse litigation and associated reputational harm which could impact confidence in the IHG brand and our ability to perform in key markets.

The Board considers reporting and insight from management, including on:

- corporate governance and regulatory developments from the General Counsel and the external Auditor;
- relevant corporate affairs topics, including briefings from external advisers;
- material litigation matters and serious operational safety and security incidents and threats;
- second-line updates on specific regulatory matters, including tax, as well as fraud risk management controls, supported by external insight and benchmarking where appropriate;
- regional trends within Regional CEO updates; and
- management strategies to procure appropriate insurance coverage, including for casualty, property, cyber and directors' and officers' liability risks.

The Executive Committee also actively monitors the management of key regulatory and/or litigation risks, including developments in cross-border data transfer regulation.

The Internal Audit plan considers regulatory management and provides independent assurance on the proportionality of controls: for example, due diligence protocols for vendors and owners, third-party guest data management and broader contract management.

Illustrative examples for 3.4.2 Additional risk attributes

Figure 17

Pearson 2023 ARA, p. 63 – Setting out the risk owner accountability

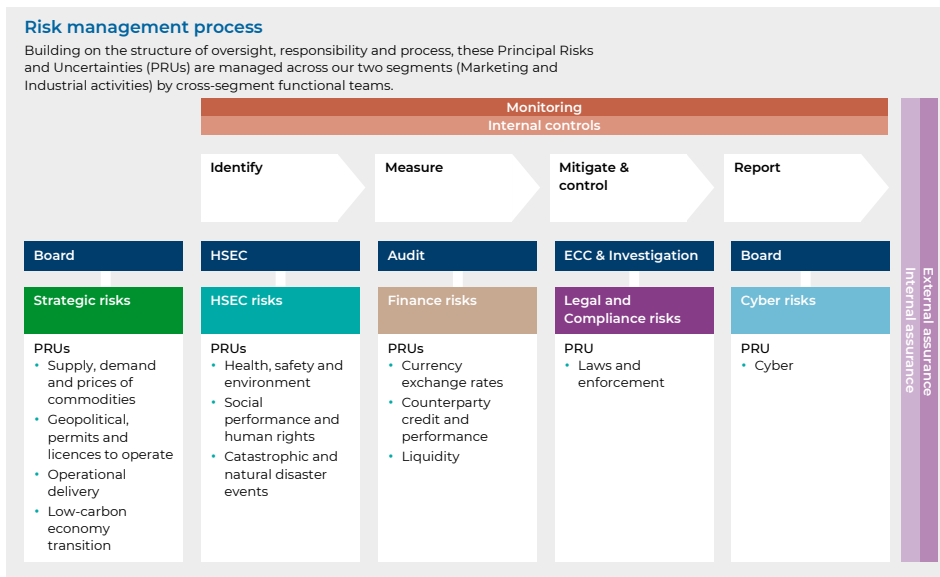
Accountability for principal risks

For each of our principal risks (shown in bold), the table below lists the accountable senior executive(s) for each sub-risk. Since 2022, the Group has created a new position of Chief Product Officer, which has led to the changes in accountability marked in the table below.

Risks	Accountability Change	Since 2022
Accreditation risk		
Political and regulatory	Chief Legal Officer and Divisional Presidents	No
Artificial Intelligence, Content and Channel risk		
Effective method of delivery (podcast, video, test, in-person, online)	Chief Product Officer and Divisional Presidents	Yes
Intellectual property protection	Chief Legal Officer and Divisional Presidents	No
Products and services – effective investment in own and third-party content	Chief Product Officer and Divisional Presidents	Yes
Balance of content creation vs content purchased	Chief Product Officer and Divisional Presidents	Yes
Artificial Intelligence, Content and Channel risk		
Effective method of delivery (podcast, video, test, in-person, online)	Chief Product Officer and Divisional Presidents	Yes
Intellectual property protection	Chief Legal Officer and Divisional Presidents	No
Products and services – effective investment in own and third-party content	Chief Product Officer and Divisional Presidents	Yes
Balance of content creation vs content purchased	Chief Product Officer and Divisional Presidents	Yes
Capability risk		
Business resilience	Chief Legal Officer and Divisional Presidents	No
Business transformation and change	Chief Executive Officer and Divisional Presidents	No
IT resilience	Chief Information Officer and Divisional Presidents	No
Safety and corporate security	Chief Legal Officer and Divisional Presidents	No
Talent	Chief Human Resources Officer and Divisional Presidents	No
Competitive marketplace risk		
Consumer learning preferences	Divisional Presidents	No
Market pricing	Divisional Presidents	No
Product differentiation	Divisional Presidents	No
Substitutes	Divisional Presidents	No
Customer expectations risk		
Customer experience	Chief Product Officer and Divisional Presidents	Yes
Accessibility	Chief Human Resources Officer, Chief Product Officer and Divisional Presidents	Yes
Data architecture and usage	Chief Information Officer, Chief Strategy Officer and Divisional Presidents	Yes
Portfolio change risk		
Achieving value on acquisitions/disposals	Chief Financial Officer and Chief Strategy Officer	No
Identification of requirements	Chief Executive Officer, Chief Financial Officer and Chief Strategy Officer	No
Integration of acquisitions	Chief Financial Officer	No
Reputation and responsibility risk		
Compliance with laws and regulations	Chief Legal Officer and Divisional Presidents	No
Cyber security	Chief Information Officer	No
Safeguarding	Chief Legal Officer and Divisional Presidents	No
Test failure	Assessment & Qualifications, English Language Learning and Workforce Skills Divisional Presidents	No
Data privacy	Chief Legal Officer and Divisional Presidents	No
Use of third parties	Chief Financial Officer and Divisional Presidents	No

Figure 18

Glencore 2023 ARA, p. 106 – Setting out the risk oversight accountability



Source: <https://www.glencore.com/.rest/api/v1/documents/static/d09d8212-4a9f-4034-b2d4-49152e5a0aff/GLEN-2023-Annual-Report.pdf>

Figure 19

Rotork 2023 ARA, p. 74 – Linking from principal risks to viability scenarios

Economic and market conditions

1. Decline in market confidence	2. Increased competition
Risk owner: Chief Executive Officer Link to strategy: [Target segments] [Customer value] [Innovative products & services] Link to viability scenario: 1: Revenue decline Likelihood: High Impact: High Trend: Decreasing	Risk owners: End Market MDs Link to strategy: [Target segments] [Customer value] [Innovative products & services] Link to viability scenario: 1: Revenue decline, 2: One-off costs Likelihood: Medium Impact: Low Trend: Decreasing
Description A decline in government and private sector confidence and spending will lead to cancellations of expected projects or delays to existing expenditure commitments. This lower investment in Rotork's traditional market sectors would result in a smaller addressable market, which in turn could lead to a reduction in revenue from that sector.	Description Increased competition on price or product offering leading to a loss of sales globally or market share.
Update This risk remains unchanged from the prior year. We continue to identify opportunities in how we can support our customers to reduce emissions and increase efficiency.	Update This risk remains unchanged since the prior year, the availability of components is recovering, demand remains strong and our Growth+ strategy has identified key areas of focus for the Group.
Key mitigating actions <ul style="list-style-type: none"> Product development and innovation to address new markets and new applications in existing markets. Geographic and end market diversification provides resilience to a reduction in any one geographic area but may not fully mitigate a change in the larger end markets. Small to mid-sized orders are generally less likely to come under pressure during uncertain economic times. We estimate that 75% of Rotork orders by value are small to mid-sized, i.e. less than £100k. Increased focus on service offerings to capitalise on increased demand for product maintenance 	Key mitigating actions <ul style="list-style-type: none"> R&D investment and organic product development, or acquisition of companies with new products, to maintain differentiation from the competition both in terms of the features and quality of our products and the services we provide. Global procurement team securing lower prices and efficiencies despite difficult market. Rotork has production or sales and service operations in many low-cost countries
Risk appetite statement We will in the long term move to increase the addressable markets which we serve.	Risk appetite statement We will invest in R&D, customer service and technology in order to retain a differentiated product portfolio. We will support this by providing a leading service solution to our customers.
Focus for 2024 Alongside the continuation of our existing key mitigating actions we will: <ul style="list-style-type: none"> Continue our investment in innovation converting the pipeline into launches Identify opportunities to support our customers to increase efficiency, aligned to the 'electrification of everything' trend 	Focus for 2024 As outlined in our Growth+ strategy, we will: <ul style="list-style-type: none"> Continue our investment in innovative products and services Focus on global key account management Continue to deliver benefits from various key programmes such as lead time reduction, global transportation and global shortages Work with our supply chain partners to build strategic partnerships Review how we deliver to customers including moving forward with our digital strategy

Strategy key
 [Target segments] [Customer value] [Innovative products & services]

Trend key
 [Increasing] [Stable] [Decreasing]

Source: <https://www.rotork.com/uploads/documents-versions/47489/1/pub082-241-00-0324.pdf>

Figure 20

Balfour Beatty 2023 ARA, p. 94 – Risk appetite rating

Risk attitude and appetite

Risks that the Group is exposed to throughout day-to-day delivery and the longer-term pursuit of strategic objectives continue to be monitored in line with appetite – and decisions taken in line with the organisation’s attitude to risk.

The Group’s risk appetite remains aligned to the Build to Last strategy, ensuring that

risk-based decision making on whether to accept or further manage risk supports the pursuit of its objectives. The strength and ongoing effectiveness of the internal control environment within the risk structure outlined on pages 145 to 151 is considered when addressing risk appetite.

The Board, its sub-committees and executive management discuss and measure the nature and extent of current and Emerging Risks faced by the Group in achieving its

long-term strategic objectives. This requires biannual review of the effectiveness of its internal control environment within the risk management structure outlined on pages 145 to 151. The outcome of this assessment represents the Group’s risk appetite and can be set out in the context of the Group’s values as shown below.

Build to Last strategy	Risk attitude	Appetite	Related principal risks
<p>Lean</p> <p>We create value for our customers and drive continuous improvement</p>	<p>Balfour Beatty remains committed to challenging ways of working to improve outcomes and become more competitive.</p> <p>The Group is prepared to accept a level of operational risk in its delivery of cost effective solutions.</p> <p>Such risks must not be at the expense of meeting customer requirements.</p> <p>The Group’s risk appetite for efficiency remains moderate.</p>	<p>M</p> <p>REMAINS MODERATE</p>	<p>7, 9, 12</p> <p>p100, p101, p102</p>
<p>Expert</p> <p>Our highly skilled colleagues and partners set us apart</p>	<p>Balfour Beatty continues to develop its expertise in engineering, computer science, robotics, data analytics, electronics and electrical and mechanical engineering to deliver the very best solutions to its customers.</p> <p>This drive for sustained innovation is undertaken with industry experts in managed and safe environments to minimise risk.</p> <p>The Group continues to have a moderate appetite for expert risk.</p>	<p>M</p> <p>REMAINS MODERATE</p>	<p>2, 3, 6, 7, 13</p> <p>p97, p97, p99, p100, p103</p>
<p>Trusted</p> <p>We deliver on our promises and we do the right thing</p>	<p>Balfour Beatty must deliver on its promises to stakeholders.</p> <p>Aligning delivery objectives to those of the customer is critical to ensuring successful outcomes – the Group strives for Right First Time delivery.</p> <p>Ensuring integrity is embedded throughout the Group and its supply chain partners is key to doing the right thing.</p> <p>The Group’s appetite for not meeting customer expectations remains low.</p>	<p>L</p> <p>REMAINS LOW</p>	<p>2, 3, 4, 5, 6, 7, 8, 9, 10, 11</p> <p>p97, p97, p98, p98, p99, p100, p100, p101, p101, p102</p>
<p>Safe</p> <p>We make safety personal</p>	<p>Conducting business in a safe way and providing a Zero Harm environment for Balfour Beatty’s people and stakeholders is paramount.</p> <p>The Group’s appetite for health and safety risk remains at zero.</p>	<p>0</p> <p>REMAINS ZERO</p>	<p>1, 7</p> <p>p96, p100</p>
<p>Sustainable</p> <p>We act responsibly to protect and enhance our planet and society</p>	<p>Balfour Beatty is committed to leaving a positive legacy for the society and communities it serves.</p> <p>The Group seeks to minimise its impact on the environment, working with supply chain partners, customers and communities to ensure its choices are sustainable, whilst delivering customer objectives, and pursuing new initiatives and technologies to achieve this.</p> <p>The Group’s appetite for risk around sustainability is moderate.</p>	<p>M</p> <p>REMAINS MODERATE</p>	<p>2, 3, 7</p> <p>p97, p97, p100</p>

Source: <https://www.balfourbeatty.com/media/5uubwxhm/balfour-beatty-annual-report-and-accounts-2023.pdf>

Figure 21

Computacenter 2023 ARA, p. 69 – Risk appetite statement

Principal risks and uncertainties continued

1. Strategic risks		1. Strategic risks continued	
<p>Alert status</p> <p>Our response continues to mature in line with market and customer changes. Increased geopolitical volatility is offset by well-managed internal responses.</p>		<p>Mitigation</p> <ul style="list-style-type: none"> Well-defined Group strategy, backed by an annual strategy process that considers our offerings against market changes New Group Portfolio Board which meets quarterly to align and define our go-to-market strategy by Service and by business line/solution area In the Managed Services Service Line, the Capabilities and Innovation function reviews the Service Line's specific needs and strategy for competitiveness and growth Location strategy coupled with well-defined business continuity processes Regular location risk monitoring covering political, economic, social, technological, legal and environmental risks 	
<p>Appetite</p> <p>Our risk appetite relating to geopolitical risk and our location strategy is balanced. By utilising multiple locations we increase the likelihood of an event or events occurring, but we reduce the impact that an event in any one location would have on the business, coupled with our business continuity strategy.</p>		<ul style="list-style-type: none"> Group Investments and Strategy Board, which considers strategic initiatives Additional measures including CEO-led country, sector and win/loss reviews 	
<p>Risks</p> <ul style="list-style-type: none"> Market shift in technology usage, making what we do less relevant or superfluous and we fail to invest appropriately to defend our competitiveness The increasingly global nature of our operations exposes us to additional and specific political and economic influences, such as geopolitical risk relating to our operational base and changes in the competitive landscape for certain business activities which attract large global competitors 		<p>Risk owners</p> <ul style="list-style-type: none"> Group Development Director Managing Director Managed Services 	
<p>Principal impacts</p> <ul style="list-style-type: none"> Reduced margin Excess operational employees 		<ul style="list-style-type: none"> Contracts not renewed Missed business opportunities 	

Source: <https://investors.computacenter.com/static-files/7a34fca6-165e-421b-8472-c75c8095b081>

Figure 22

BT Group 2024 ARA, p. 63 – Risk appetite statement

Strategy, technology and competition

Sponsor: Chief Financial Officer

What this category covers

To deliver value to our stakeholders and achieve our strategic objectives, we must carefully manage risks around economic uncertainty, intensifying competition and rapidly changing customer and technology trends. If we adopt the wrong strategy, fail to incorporate our strategy into our business plans or don't effectively implement it, we could become less competitive and hinder the creation of long-term sustainable value.

Our risk appetite

Our risk appetite sets our tolerance for managing 'internal' risks associated with this category. We measure and track this through specific metrics. We also qualitatively assess the clarity of our strategy, robustness of our strategic analysis and whether our business and financial plans align with our strategy. Doing this helps us make robust strategic choices and effectively implement them – to stay competitive and grow value for our stakeholders.

Examples of dynamic risks

Point risks:

- Macroeconomic environment factors like high inflation, high interest rates and reduced customer confidence may lower demand, increase customers' price sensitivity and drive up costs.
- Intensifying competition in retail and wholesale markets could increase churn and affect our market share.
- Disintermediation by hyperscalers could result in loss of market share and weakened customer relationships.
- Slower than planned progress on key programmes could limit our ability to deliver our strategy and growth ambitions.

Emerging risk:

- Failing to harness AI technologies to drive efficiencies and generate value could make us less competitive.

Examples of what we do to manage these risks

- We research, analyse and monitor economic, customer, competitor and technology trends to inform our strategy.
- The *Executive Committee* and Board regularly review performance against our strategic priorities and targets.
- The *Executive Committee* and Board discuss key strategic topics throughout the year.
- BT Investment Sub-Committee considers our investments to make sure they are aligned to our strategy.

Scenarios considered in viability analysis

Hyperscalers strategically entering our markets through direct initiatives.

Competitive pressures from alternative FTTP network providers continue to intensify.

Stakeholder management

Sponsor: Corporate Affairs Director

What this category covers

Stakeholder management, built on trust, is essential to us achieving our ambitions. We engage with stakeholders fairly and transparently to maintain strong, sustainable relationships and manage reputational risks. We also consider risks around using and selling emerging technologies, environment, social and governance factors, and customer fairness.

Our risk appetite

We recognise the importance of strong stakeholder relationships and consider them when setting strategy and making decisions. We aim to balance our purpose and ambition with commercial choices we think are reasonable. At times this creates tensions when weighing up options: price rises to sustain investment, the markets we operate in, who we buy from and sell to, the way we use and develop technology and how we use data.

We want to keep being sector leader on reputation and trust among professional opinion formers, and stay in our top quartile position on ESG.

Examples of dynamic risks

Point risks:

- Protecting our customers' interests while migrating to digital products and closing legacy networks.
- Continued geopolitical tensions needing extra focus on reputational risks associated with our global operations.

Emerging risks:

- Rapid advances in AI with associated stakeholder scrutiny on things like data ethics and reskilling.
- Climate change, and perceptions of our sector's role in carbon emissions. See our Task Force on Climate-related Financial Disclosures (pages 71 to 80).

Examples of what we do to manage these risks

- Our Manifesto (pages 34 to 39) sets out our commitment to growth through responsible, inclusive and sustainable technology. The *Responsible Business Committee* provides Board-level governance.
- We monitor the media, and track our reputation across our main stakeholder groups.
- We engage with stakeholders to build strong relationships. See pages 40 to 45 for details.
- We have robust product, services and communication plans to improve customer outcomes.

Scenario considered in viability analysis

Potential changes in Government policy affecting our investment and commercial ambitions.

Source: <https://www.bt.com/bt-plc/assets/documents/investors/financial-reporting-and-news/annual-reports/2024/2024-bt-group-plc-annual-report.pdf>

Figure 23

RHI Magnesita 2023 ARA, p. 52 – Remaining within risk appetite

1. Macroeconomic and geopolitical environment

Link to strategy



Target risk appetite



KPIs

Revenue, Adjusted EBITA margin, Adjusted EPS, ROIC

Internally monitored metrics

Key macroeconomic and financial market indicators, steel and cement forecasted production.

Risk description

Changes in the global economic environment, financial markets conditions and adverse geopolitical developments may have an impact on the Group's revenue and profitability.

The macroeconomic environment changes leading to sales volume reductions can arise from industrial factors or from wider global issues, such as a global economic downturn or global logistic challenges.

The demand for refractory products is directly influenced by steel, cement and non-ferrous metal production, metal and energy prices and the production methods used by customers.

Due to the Group's cost structure, fluctuations in sales volumes have an impact on the utilisation of production capacities and consequently on the Group's profitability and gearing.

Examples of specific risks:

- Decreasing investment in customers' infrastructure projects (therefore reducing steel and cement demand) leading to lower refractory consumption and depressed sales volumes.
- Customers focusing on lower-cost and more commoditised refractories.
- Lower sales volumes leading to lower fixed cost absorption.
- Increasing prices of core resources and supplies (e.g., energy, freight and packaging).

Risk mitigation

- Initiatives to increase the Group's resilience, through establishing leaner processes and lower fixed cost structures whilst increasing the Group's market share and the value for our customers.
- Diversification of geographies and industries.
- Close monitoring of production costs fluctuations to guarantee the expected profitability.
- Price increase initiative to pass inflationary costs to customers.
- Early leading indicators to ensure identification of emerging macroeconomic trends.
- Treasury Policy and usage of financial instruments to mitigate risk exposure to financial markets.
- Agile, experienced, and solution-focused management teams who can respond quickly and innovatively to challenges.

Risk movement

During 2023, the macroeconomic environment continues to be challenging for the refractory industry. The refractory market experienced a drop in customer demand in most markets.

Events such as the Russia-Ukraine conflict generated higher risks relating to input costs such as energy and through sanctions restrictions, especially in late 2023 when the mixes product group of the Group was subjected to specific EU sanctions in respect of Russian sales.

Disruption in the global logistics mechanisms, whilst less marked than in 2022, still presented a risk as demonstrated by disruptions to Red Sea shipping lanes restrictions in late 2023.

The risk appetite remains high (no changes from 2022). The risk score is within the risk appetite but has the potential to exceed it and is closely monitored.

Source: <https://ir.rhimagnesita.com/wp-content/uploads/2024/02/rhim-ar-fy-2023-compressed.pdf>

Illustrative examples for 3.5.1 Aspects of current practice that will need to evolve

Figure 24

BT Group 2024 ARA, p. 100 – Grouping of audit committee activities

Audit, risk and internal control continued
Audit & Risk Committee Chair's Report continued

Overview of the year

Focus	Considered by the Committee					
	2023 Apr	May	Jul	Sep	Oct	2024 Jan
Financial reporting						
– Results/trading updates and accounting judgements	█	█	█		█	█
– Annual Report 2023	█	█				
– Regulatory financial statements			█			
– Going concern assessment		█			█	
– Viability statement		█				
Litigation and major contentious matters		█	█	█	█	█
Internal controls over financial reporting		█	█		█	
GRCs and CFU risk reviews: point and emerging risks	█	█		█		█
Report from Openreach Board, Audit, Risk & Compliance Committee chair			█		█	█
Compliance with Code requirements – risk management framework		█				
Ethics & compliance						
– Ethics & compliance programmes		█	█		█	█
– Speak Up (whistleblowing) reports		█	█		█	█
Internal audit						
– Internal audit report		█	█		█	█
– FY24 group internal audit plan and approach	█					
– Group internal audit charter		█				
– Effectiveness						█
External audit – KPMG						
– External audit report	█	█			█	█
– External audit plan			█			
– Audit and non-audit fees		█	█		█	
– Effectiveness		█		█		
– Independence and reappointment		█				

Source: <https://www.bt.com/bt-plc/assets/documents/investors/financial-reporting-and-news/annual-reports/2024/2024-bt-group-plc-annual-report.pdf>

Figure 25

Inchcape 2023 ARA, p. 63 – Demonstrating the cadence of monitoring

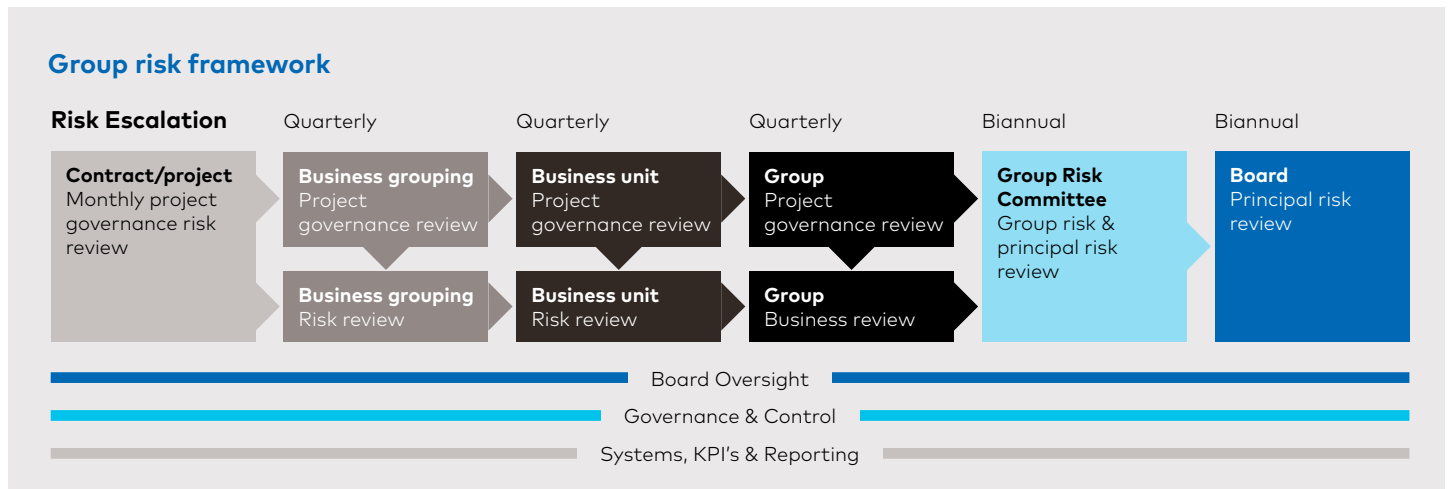
The Board is ultimately accountable for the system of risk management and internal control, and for managing risks to be within acceptable levels. During 2023, the Board, Audit Committee, and Group Executive Team reviewed the following topics relating to the Group's principal risks:

	Board	Audit Committee	Group Executive Team
Q1	CROs quantification and scope 3; legal and regulatory; risk policy; capital structure; viability; M&A; and Derco integration	Internal controls (financial reporting, fraud, technology systems risks); viability; and Derco integration	EV transition (scope 1 & 2, EV strategy); political (high risk markets); HSE due diligence (M&A); principal and emerging risks; business continuity; people (leadership); VLS; and Distribution Excellence
Q2	Strategy: macro and industry trends; EV and industry decarbonisation; Distribution Excellence; VLS; mobility company partners; EV transition; and climate change	Cybersecurity; internal controls (financial reporting, fraud, and technology systems risks); and Derco integration	Cyber; EV transition (portfolio choices); people (health & wellbeing); digital (S&OP, and data analytics platform); Responsible Business; business resilience; VLS; Distribution Excellence; Global Business Services (GBS); principal and emerging risks; and strategy
Q3	Half-year risk review; Derco integration; Responsible Business; and cybersecurity	Half-year risk review; internal controls (financial reporting, fraud, and technology systems risks); GBS; and Derco integration	Digital (enterprise resource planning, and digital experience platform); people (health & wellbeing, Inclusion and Diversity, and leadership); ESG; and financial reporting (transfer pricing)
Q4	HSE; digital; people; strategy; supply chain disruption; principal and emerging risks; and risk appetite	Cybersecurity; internal controls (financial reporting, fraud, and technology systems risks); GBS; Derco integration; and risk management effectiveness	Cyber; AI; EV transition (materiality assessment, and EV procedures); principal and emerging risks; people (colleague engagement); global policy standards; M&A; strategy; distribution agreements; legal & regulatory compliance (Code of Conduct); and Responsible Business (Planet)

Source: <https://www.inchcape.com/wp-content/uploads/2024/03/2023-Annual-Report-Accounts.pdf>

Figure 26

John Wood Group 2023 ARA, p. 83 – Demonstrating the cadence of monitoring



Source: https://www.woodplc.com/_data/assets/pdf_file/0026/256751/John_Wood_Group_PLC_Annual_Report_and_Financial_Statements_2023.pdf

Illustrative examples for 3.5.2 Good practice governance reporting

Figure 27

(Extracts referred to in section 3.5.2.1 General)

Rentokil Initial 2023 ARA, p. 123

The Audit Committee receives regular reports from the Chief Financial Officer and the Director of Internal Audit & Risk on financial controls and process improvement programmes, including:

- ▶ An annual report on the overall status of the control environment in the Group, including the results of testing and reports on identified areas of weakness in controls;
- ▶ Action plans on control environment improvements and updates on their implementation;
- ▶ Updates on control weaknesses and planned actions to prevent a reoccurrence;
- ▶ Periodic reports from regional and Group finance executives, and Internal Audit; and
- ▶ Updates on the SOX implementation programme.

During 2023, the Audit Committee was updated on the risk and control environment in the main businesses, as well as the Regional Finance Directors’ assessment of the quality and priorities of the Finance function in the relevant part of the business. Audit Committee members received reports from the Regional Finance Directors for the UK & Sub-Saharan Africa region and the Pacific region, with other regional updates provided as part of the Board agenda. This provides a high-level insight for the Audit Committee on potential risks.

The Audit Committee also receives the minutes of the Group Risk Committee. The Group Risk Committee comprises the key functional and operational senior managers, and considers the risk framework, and key and emerging risks. Where appropriate, items that are raised as significant or emerging issues by the Group Risk Committee are reflected in adjustments to the control environment. In 2023, some control issues were experienced including:

- ▶ A colleague had their IT user credentials compromised. No data was lost and there were no further instances of weaker security protocols;
- ▶ Three businesses performed work without authorisation under the Group’s Pink Note process. This was subsequently rectified and guidance reissued; and
- ▶ A payment fraud in our Australian business of immaterial scale to the Group.

Legal & General Group 2023 ARA, p. 93

2023 activity

(...)

Alongside the Group Chief Risk Officer's report, the Committee is provided with management information on risk appetite, comparing actual positions relative to the Group's risk appetite statement and quantitative analysis of the Group's exposures to financial and operational risks, including risk-based capital requirements in relation to the core risks implicit in the Group's businesses. The Committee also receives an assessment of the overall profile of conduct risks for the Group; analysis and trends in complaints data and a suite of customer service metrics designed to enable the Committee to assess the management of the customer journey.

Severn Trent 2023 ARA, p. 157

The Committee received half-yearly reports from the Head of Risk, detailing the significant risks and uncertainties faced by the Group. Each risk submitted for review includes an assessment of the overall risk status, status of the control environment and a summary of the risk mitigation plan to take the risk to the target risk position, which needs to be in line with the risk appetite. The risk mitigation strategies include action plans to improve controls where this has been assessed as necessary and determines whether actions are on target and with the correct prioritisation in place. Further details of the Group's risk management framework, controls and Principal Risks can be found in the Strategic Report on pages 95 to 101.

The Weir Group 2023 ARA, p. 101

Compliance scorecard

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, cybersecurity, 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 and employee costs. The scorecard process has been extended in recent years to cover areas of non-financial reporting such as scope 1&2 emissions and Total Incident Rate reporting. 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 audits. 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 Audit Committee 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.

PPHE Hotel Group 2023 ARA, p. 127

Enterprise Risk Management (ERM)

The Board is responsible for risk management with guidance from the Audit Committee. A standing agenda item in every Audit Committee meeting is consideration of the Company's risk register, with the main focus on key risks.

The Audit Committee monitors the Company's risk management system and controls to review their effectiveness.

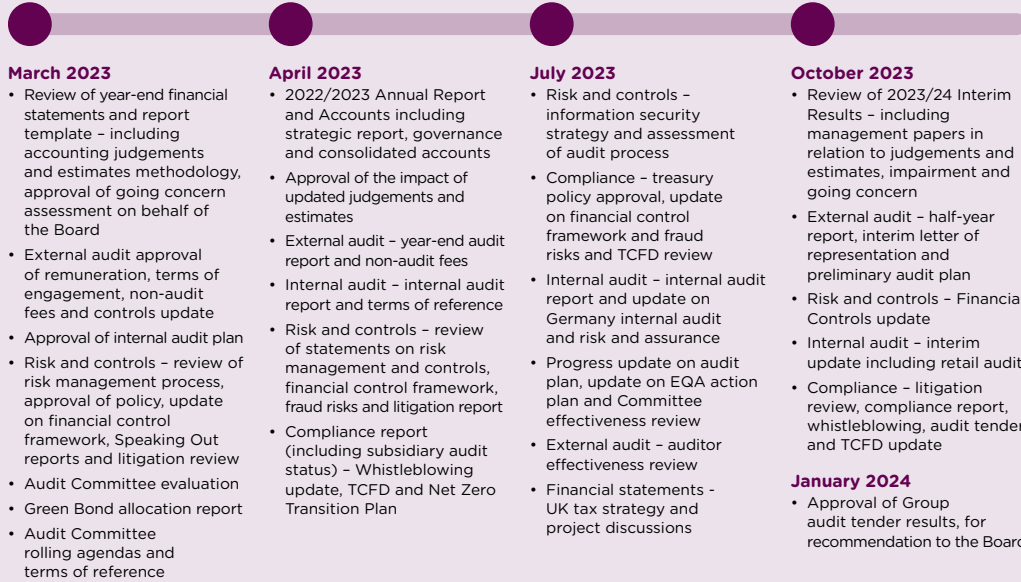
The process for evaluating the effectiveness of the ERM system and controls requires the output of the system to be benchmarked against similar organisations, using publicly available information. It is also benchmarked against reports and publications from appropriate professional bodies and institutions. The formal assurance process takes place annually.

Figure 28

Whitbread 2024 ARA, p. 121 – Governance actions undertaken post year-end

Main activities during the year

In 2023/24, the Audit Committee's work covered internal controls, risk management, internal audit, external audit and financial reporting. The details of the matters discussed at Committee meetings are shown below.



Main activities post financial year

March 2024

- Review of year-end financial statements and report template – including accounting judgements and estimates methodology, approval of going concern assessment on behalf of the Board
- External audit – audit update report, AQR output review, approval of remuneration, non-audit fees and UK Corporate Code update
- Internal audit – approval of plan and update on recent internal audits
- Risk and controls – approval of risk management policy and management framework, update on financial control framework and cyber risks
- Audit Committee evaluation
- Compliance report (including subsidiary audit status) and TCFD

April 2024

- 2023/2024 Annual Report and Accounts including strategic report, governance and consolidated accounts
- Approval of the impact of updated judgements and estimates
- External audit – year-end audit report and non-audit fees
- Internal audit – internal audit report and terms of reference
- Risk and controls – review of statements on risk management and tax controls and litigation report
- Compliance report – whistleblowing and TCFD update

Source: https://cdn.whitbread.co.uk/media/2024/05/Whitbread-PLC-Annual-Report-and-Accounts-2023_Single_pages-1.pdf

Figure 29

Lloyds Banking Group 2023 ARA, p. 102-106 – Detailed narrative setting out the actions of the risk committee

Board Risk Committee report

Operational resilience and sound risk management are fundamental to the strength of the Group

Catherine Woods
Chair, Board Risk Committee



Delivery of the Group's strategic and cultural transformation will help strengthen the management of risks which have the potential to impact the Group and its customers.

Key activities in 2023

- Overseeing the Group's strategic transformation and management of change and execution risks
- Considered the impacts of the rising cost of living, higher interest rates and inflation, macroeconomic uncertainties, and geopolitical risks on both the Group and its customers
- Overseeing the embedding of the Group's operational risk and control framework and discussing evolution of the broader risk framework
- Assessing the management of operational resilience risks, including cyber, supply chain management and technology risks, data risks and artificial intelligence
- Overseeing management of financial crime risks and consumer fraud
- Overseeing continued progress on the Group's climate risk framework and net zero transition
- Reviewing management of the Group's funding and liquidity risks including structural hedge activity
- Assessment of key emerging risks and oversight of strategic risks

Source: <https://www.lloydsbankinggroup.com/assets/pdfs/investors/financial-performance/lloyds-banking-group-plc/2023/q4/2023-lbg-annual-report.pdf>

Risk type	Key issues	Committee review and conclusions
Operational resilience (IT resilience, cyber, and supplier management)	Operational resilience remains one of the Group's most important non-financial risks. We continue to enhance our resilience to better serve customers and to address regulatory priorities.	<p>The Committee has received reports on the Group's overall maturity against a suite of operational resilience capabilities and on the refinement of the impact tolerances of important business services. The Committee has also reviewed Group-wide self-assessments covering progress on the enhancements needed to ensure our important business services can be recovered within impact tolerance by March 2025 (in response to regulatory policy statements on operational resilience published in March 2023). Close attention has been paid to the Group's management of its contracts with its suppliers to ensure resilience of services to customers. Given the significance of the risk to the Group, the Committee is supported by the IT and Cyber Advisory Forum specifically focused on IT and cyber risks.</p> <p>Conclusion: The Committee has requested further specific updates on the progress of the Group-wide Operational Resilience Programme, the impact of investment on operational resilience and the way in which data is used to support management decisions around operational resilience.</p>
Data risk	Data strategy plans to remediate legacy and emerging risk challenges in the Group's data control environment to enable strategic objectives.	<p>Data risk continues to be an area of significant regulatory and media attention, particularly relating to new technologies such as artificial intelligence. Frequent updates have been provided to the Committee on the progress of the data strategy in response to legacy and emerging data risk challenges including on data quality and lineage controls and enhancing the Group's governance framework e.g. around Data Ethics.</p> <p>Conclusion: The Committee continues to be supportive of the data strategy and approach, recognising the complex roadmap of initiatives planned over a number of years. Delivery of the data strategy is critical, given data is a key enabler for good customer outcomes and the overall Group strategy.</p>
People and health and safety risk	Managing people risks arising from the cultural transformation of the workforce will be critical to ensure we attract and retain the right skills and capabilities to deliver our strategy.	<p>People risk remains a key focus of the Committee, reflecting the scale and complexity of change required to the skills composition and size of our workforce. The Committee considered the current, emerging and horizon risks arising from the people plan and how these would be effectively monitored and managed with continued focus on culture, capability and capacity, colleague proposition, health and safety and wellbeing. The Committee also considered a deep dive on health and safety which highlighted enhancements to the framework, bringing more rigour and management focus to ensure we create a safe and healthy workplace.</p> <p>Conclusion: The Committee supports the people plan and acknowledges that delivering the plan is critical to increasing our capability and capacity to deliver change faster as we move purposefully towards a high performing culture. People risk will remain a key area of focus in 2024 as the transformation journey continues.</p>
Strategic transformation oversight	Risks associated with the extensive current and future Group strategic change agenda, recognising challenges faced in ensuring both successful delivery and implementation of change.	<p>The Committee has reviewed the portfolio performance on a regular basis, focusing on the Board metric outcomes and underlying deliverables, which supports the Group's strategic growth ambitions. The focus for 2023 has centred on embedding the new platform-based operating model and ensuring management is learning from the root causes of any delivery delays. The Committee, with the IT and Cyber Advisory Forum, also increased its monitoring of the safe delivery of change for important business services with dedicated deep dives undertaken throughout 2023, which is critical to ensure we avoid customer harm and minimise operational incidents.</p> <p>Conclusion: The Committee will continue to focus on the management of change and execution risk within appetite and on monitoring the outcomes being achieved. The Committee will review how the expected evolution of the platform model and agile change delivery approach is undertaken in 2024. Enhancing resilience in relation to our important business services remains a priority, ensuring that any strategic transformation delivered does not cause customer harm or compromise our operational resilience posture.</p>

Figure 30

(Extracts referred to in section 3.5.2.2 Risk management and risk-management related)

Morgan Sindall Group 2023 ARA, p. 128

Risk review

In August and December 2023, the committee carried out on behalf of the Board a robust assessment of the Company's emerging and principal risks. The divisions, IT team and risk committee reviewed their risk registers to enable the committee to conduct a formal appraisal of the Group and divisional risk registers. The registers include the controls and mitigations in place for principal and emerging risks and indicators of any changes in risk level that may impact our strategy over the medium to longer term. An overview of the risk management process is described on page 66. As part of its review, the committee conducts deep dives into key topic areas relating to our principal risks to discuss whether risk levels are still aligned with our strategy and risk appetite. In 2023, the deep dives focused on:

- ▶ The potential macroeconomic effect on future residential portfolios (principal risk B, page 71);
- ▶ The impacts of construction inflation and commodity availability (principal risk A, page 70);
- ▶ Supply chain solvency given continued pressures from the economic climate (principal risk E, page 73); and
- ▶ A review of our latent defect risk, taking into consideration our estimation of the costs of applying the principles of
- ▶ The Building Safety Act and the developers' pledge across Partnership Housing and Urban Regeneration (principal risk I, page 76).

AstraZeneca 2023 ARA, p. 95

Risk identification and management

(...)

The Committee is updated on key active and emerging risks facing the Company through a quarterly risk management report from the CFO. The likelihood of each of the risks materialising and its potential impact was monitored by the Committee and the reports from the CFO enabled the Committee to track the trend applicable to each risk compared to the previous quarter. The composition and profile of these risks informs the Committee's agenda of in-depth sessions. For example, an upward trend, in terms of the likelihood and potential impact of the risk, was noted for the key active risk relating to IT, cyber risk and data security, therefore the Committee spent additional time with representatives from the IT function to understand those risks and the actions being undertaken to mitigate them.

Drax Group 2023 ARA, p. 95

Internal control

(...)

Annually, the Audit Committee review and challenge an assurance map prepared by management detailing the level of assurance obtained for each of the Group's Principal Risks across different lines of defence, including both internal and independent external assurance. This review considers whether any increase in the risks facing the Group require a respective enhancement in the level of assurance obtained. For example, an updated approach to HSE assurance was recently approved by the Audit Committee, including internal peer reviews, an external implementation review of Group HSE management systems in the business units and external assessments of compliance with local HSE legislation and regulation. Refer to page 67 for further information.

Smith+Nephew 2023 ARA, p. 117

Internal control

Internal audit

(...)

During the year, the team completed 35 audits and reviews across the Group. These covered significant aspects of all 11 Principal Risks and included: financial controls effectiveness reviews across the EMEA, APAC, US and LATAM regions; IT and various programme assurance reviews ranging from IT disaster recovery planning and cyber maturity; and an ERP pre-implementation review in Japan. Group-level reviews included enterprise risk management effectiveness, business continuity management arrangements, ESG governance, field inventory controls, trade compliance activities, 12-Point Plan governance and fraud risk management effectiveness. Management have taken swift action to implement Internal Audit's recommendations. The team was able to travel to a number of locations, following the relaxing of Covid-related restrictions and there was continued use of data extraction and analysis techniques during all work.

Figure 31

(Extracts referred to in section 3.5.2.3 Controls-related)

Lloyds Banking Group 2023 ARA, p. 93

Control effectiveness review

All material controls are recorded and assessed on a regular basis in response to triggers or at least annually. Control assessments consider both the adequacy of their design and operating effectiveness. Where a control is not effective, the root cause is established, and action plans implemented to improve control design or performance. Control effectiveness against all residual risks is aggregated by risk category, reported and monitored via the monthly Key Risk Insights or Consolidated Risk Report (CRR). The Key Risk Insights/CRR are reviewed and independently challenged by the Risk division and provided to the Risk Division Executive Committee and the Group Risk Committee. On an annual basis, a point in time assessment is made for control effectiveness against each risk category and across the sub-groups. The Operational Risk System, Key Risk Insights or CRR are the sources used for this point in time assessment and a year-on-year comparison on control effectiveness is reported to the Board Risk Committee and the Board.

NatWest 2023 ARA, p. 111

Theme	Principal areas of focus	Outcomes
Early event escalation	To monitor control incidents captured by the internal	The committee received bi-annual updates on the volumes and nature of the most significant control incidents escalated via the internal early event escalation process and any common themes. All Board directors were alerted to the most significant events throughout the year. A reduced volume of Major events was noted in 2023.

Taylor Wimpey 2023 ARA, p. 122

IT Operating environment

(...)

Other improvements included:

- ▶ Increased resources and improved approach to working with projects to ensure security is embedded by design.
- ▶ Extending our security controls to cover a wider range of IT services.
- ▶ A step improvement in monitoring vulnerabilities and remediating them promptly.
- ▶ Introducing a more extensive testing regime for security vulnerabilities in legacy systems.

Plans for further enhancements to cyber resilience during 2024 include:

- ▶ Further development of our business continuity readiness plan, being undertaken by Internal Audit.
- ▶ Transition to a new approach for managing IT services within the Group, including new security services.
- ▶ Improving our monitoring of key suppliers' cyber security ratings.

bp 2023 ARA p. 102

Internal controls

(...)

Undertook a deep-dive on significant deficiencies and control environment, with a focus on IT user access and journal controls. The committee focused on mitigating measures, ongoing remediation work and challenged management on the timeline for the development of more enduring controls

Ocado Group 2023 ARA, p. 150

Risk management and internal controls

(...)

The Finance transformation focus of the past two years through the Evolve programme meant that significant progress has been made to build the necessary Finance capabilities, reduce reporting risks and mature the financial control environment. Further improvements in other key areas including payroll, treasury and business planning and forecasting processes has meant tighter oversight of spending and liquidity management for the Group.

Reviewing the effectiveness of risk management and internal control

(...)

In addition to these routine reviews of risk management and internal control, and in line with the provisions of the UK Corporate Governance Code, a formal annual assessment is performed by the Committee on behalf of the Board. This assessment draws on an independent summary produced by the Director of Internal Audit, utilising the Guidance on Risk Management Reporting, Internal Control and Related Financial and Business Reporting issued by the FRC in September 2014, an analysis of audit findings through the year, and feedback obtained from formal representations made by senior management and Finance teams. The 2023 assessment concluded that controls were generally operating effectively, despite internal audit findings identifying a continued dependence on manual controls in some core processes, and reliance on the detective controls delivered through the valuation process. These improvement areas are recognised by the Board, with various workstreams and improved automation planned to address them over the medium-term. Following its processes of continuous review and consideration of the annual summary report, the Committee has concluded that the Group's systems of risk management and internal control continue to be broadly effective and appropriate.

Figure 32

(extracts referred to in section 3.5.2.4 Level of confidence)

Internal control

The Group has a well-defined system of internal control which has been in place for the year under review and up to the date of approval of the Annual Report, supported by policies and procedures and documented levels of delegated authority which underpin decision-making by management. These internal controls operate as important mitigations of the risks identified via the Group's risk management processes. Therefore, the effective design and operation of these internal controls is critical to the achievement of the Group's strategic aims. Annually, the Audit Committee review and challenge an assurance map prepared by management detailing the level of assurance obtained for each of the Group's Principal Risks across different lines of defence, including both internal and independent external assurance.

This review considers whether any increase in the risks facing the Group require a respective enhancement in the level of assurance obtained. For example, an updated approach to HSE assurance was recently approved by the Audit Committee, including internal peer reviews, an external implementation review of Group HSE management systems in the business units and external assessments of compliance with local HSE legislation and regulation. Refer to page 67 for further information.

The Audit Committee approves and oversees a programme of internal audits covering all aspects of the Group's activities on a rotational basis, following an assessment of the key risks facing the business. Refer to page 143 for further information on this programme of work. The majority of internal audits are performed by KPMG, who provide a fully outsourced internal audit function to the Group, reporting to the Audit Committee. For some specialist areas, such as HSE, expert auditors may be employed to supplement this work.

The findings and recommendations from each internal audit are distributed to members of the Executive Committee and the Audit Committee. Where weaknesses are assessed, these are investigated and the impact on the business is identified, with remediation actions established. This is also reported to the Audit Committee. None of the findings reported during 2023 were individually or collectively material to the financial performance, results, operations, or controls of the business.

Internal controls

The Committee received quarterly updates of the self-attestation of compliance with the Group's financial and IT general control frameworks, including details of control failures (all immaterial during 2023), their remediation and independent reviews of control evidence.

The Committee noted the extension of the formal control framework to include key non-financial information disclosed. The controls reliance approach on GBS controls adopted by the external auditors provided additional assurance on the centralised GBS controls to the Committee in this regard.

Based on these quarterly updates, and the reports from the internal and external auditors, the Committee is satisfied that the Group's internal controls operated effectively throughout the year, with no occurrence of material weaknesses. Controls relating to Compliance are covered in the paragraph below.

Compliance, including speaking up and fraud

The Committee reviewed update reports on the results of the global compliance programme and the speaking up process. The results of the global business risk assessments performed (jointly by the Group's compliance team and internal audit) across a number of key global markets were considered and concluded that an ethical business culture exists. The key themes arising from these risk assessments related to third party risk management (i.e. due diligence and contracting) and interactions with healthcare professionals (i.e. medical samples). These are being addressed through training and implementing new and refreshed policies and procedures. Following the completion of the assessment of the initial selected markets, the assessment process will be cascaded to cover all markets during 2024.

(...)

Phoenix Group Holdings 2023 ARA, p. 97

Internal controls

The Committee, alongside the Risk Committee, supports the Board in ensuring a robust system of internal control and risk management is in place across the Group. The Committee receives reports from the Group Head of Internal Audit on the status of the control environment and management of the Group's principal risks and controls across the Group's Risk Universe.

The Committee also considers bi-annual Internal Control Self-Assessment reports in which Line 1 risk owners self-assess the design and operation of their control environments. These assessments are independently validated by Line 2 (Risk) and supplemented by an Annual Internal Control Environment Opinion Report from Line 3 (Internal Audit).

During 2023, the Committee regularly challenged Management to ensure, where any control weaknesses were identified, that there are robust and timely action plans to address these. In performing this review and challenge of the control environment, the Committee has assessed and confirms that in 2023 it has complied with Principle O and Provisions 25 and 29 of the 2018 Code.

Looking ahead to 2024, the Committee will maintain its scrutiny of the Group's control environment, including overseeing necessary modifications to the Internal Control Framework to meet the new requirements of the 2024 Code.

Howdens 2023 ARA, p. 139

Independent assurance

The Committee assessed the coverage of independent assurance by reviewing the annual internal audit plan against the Group's key controls.

Morgan Sindall Group 2023 ARA, p. 129

Review of internal controls

The committee reviewed the effectiveness of our system of internal controls which is described in the panel on the right. The review included assessing the relationship between the internal and external audit functions, the results of internal audit work, and the overall effectiveness of the internal audit process. The committee noted that, although many of the key components of the draft Companies (Strategic Report and Directors' Report) (Amendment) Regulations were withdrawn by the government in October 2023, the proposal for an explicit statement by directors on the effectiveness of material internal controls remains. Thus, the internal audit function will continue to test the robustness of financial internal controls, as well as expand their focus to internal controls relating to non-financial reporting, specifically relating to sustainability. In addition to internal audits, a biannual self-assessment process was launched at the half year to ensure that each division takes full ownership of its own internal controls.

Any significant control deficiencies which arise from the self-assessment process are documented with a defined remediation plan and target completion date, as part of the declaration submitted by each divisional finance director.

This process will prepare directors at Group level when the time comes for them to make their explicit statement on the effectiveness of the Group's internal controls.

Travis Perkins 2023 ARA, p. 104

In 2023, particular Audit Committee focus has been on continuing management initiatives to improve the internal financial control environment. There are a number of system replacements in progress, including Apex, which will deliver a new finance system, as well as enhancing and improving the Group's control framework to lead to greater consistency and automation of controls. An independent assurance provision has been procured from PwC to underpin the plan for assuring Apex. The assurance plan has been reviewed by the Audit Committee. Regular reports on results were presented to both the Apex steering committee and the Audit Committee throughout 2023 and progress will continue to be monitored in this way in 2024. Reviewing such major system transformation programmes will also remain an area of focus for the Internal Audit function. It is also the case that all major internal assurance processes, including operational compliance, health and safety and internal audit, track control improvement actions to completion, which is a core part of the continuous improvement of controls.

Authors



Mala Shah-Coulon

Associate Partner,
Governance and Public Policy,
EY UK
mshahcoulon@uk.ey.com
+ 44 20 7951 0355



Maria Keĝa

Director,
Governance and Public Policy,
EY UK
mkepa@uk.ey.com
+ 44 7795 645183

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 organization, 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. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP

The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place, London, SE1 2AF.

© 2024 Ernst & Young LLP. Published in the UK.
All Rights Reserved.

EYSCORE 007009-24-UK

UKC-035191.indd (UK) 08/24. Artwork by Creative UK.

ED None



In line with EY's commitment to minimise its impact on the environment, this document has been printed on paper with a high recycled content.

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young LLP accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

ey.com/uk