



On track for Provision 29 compliance

Addressing the new risk
management and internal control
requirements of the 2024
UK Corporate Governance Code

July 2025



The better the question. The better the answer.
The better the world works.



Shape the future
with confidence





Contents

1. Introduction	2
2. Steps companies were taking in 2024	4
2.1. Common understanding	4
2.2. Planning for Provision 29 compliance	5
2.3. Revisiting principal risks	7
2.4. Identifying material controls	10
2.5. The magic number	16
2.6. Dynamism	17
3. Getting the foundations right	18
3.1. Financial reporting controls	19
3.2. IT general controls	21
3.3. Non-financial reporting	21
3.4. Failure to prevent fraud	22
3.5. Control self-assessments	24
3.6. Implementation of GRC tools	24
3.7. Investment in second-line capabilities	25
4. What are companies focusing on in 2025	26
4.1. Document and formalise material controls	26
4.2. Agree confidence levels	27
4.3. Agree sources of evidence	28
4.4. Determine monitoring and review activities	30
4.5. Perform a dry run	31
4.6. Artificial intelligence (AI)	31
5. Reporting recommendations	34
5.1. Introduction	34
5.2. Risk governance framework	36
5.3. Other features of the risk management and internal control framework ..	38
5.4. Risk management process	38
5.5. Risk identification and evaluation	41
5.6. Risk responses	42
5.7. Board monitoring activities	44
5.8. Board review activities	46
5.9. The directors' declaration	46
Appendix: Illustrative examples	48

1. Introduction

Last year, much energy was devoted by companies to deciphering the intent of revised Provision 29 of the 2024 UK Corporate Governance Code (the Code) to ensure their approaches to implementing this Code change were appropriately focused. Boards, risk, control and internal audit teams embarked on a journey of introspection.

At the beginning of this journey was a sense of initial scepticism and, to some extent, frustration with the lack of prescription inherent in the very flexible and principles-based nature of Provision 29.

A year on, there is a growing sense of opportunity.

These observations are based on our extensive engagement over the last 15 months, including more than 100 meetings with commercial listed companies across various industries. We convened peer-to-peer roundtables, had one-on-one discussions and delivered targeted board update sessions to help management and boards navigate the new requirements. Our work has helped companies to clarify and refine their thinking and also fostered valuable peer networks for sharing emerging practices.

Leading companies which embraced the flexibility are now well progressed on their journey to compliance, whilst those still in earlier stages of preparation face a widening gap. There is resounding agreement among these leaders that Provision 29 has provided a trigger or a mandate to do more than just think about enhancing the transparency of reporting.

Whilst there has rightly been an aversion to throwing the baby out with the bath water, and companies are keen to leverage existing disciplines and systems, so far, preparing for Provision 29 has helped:

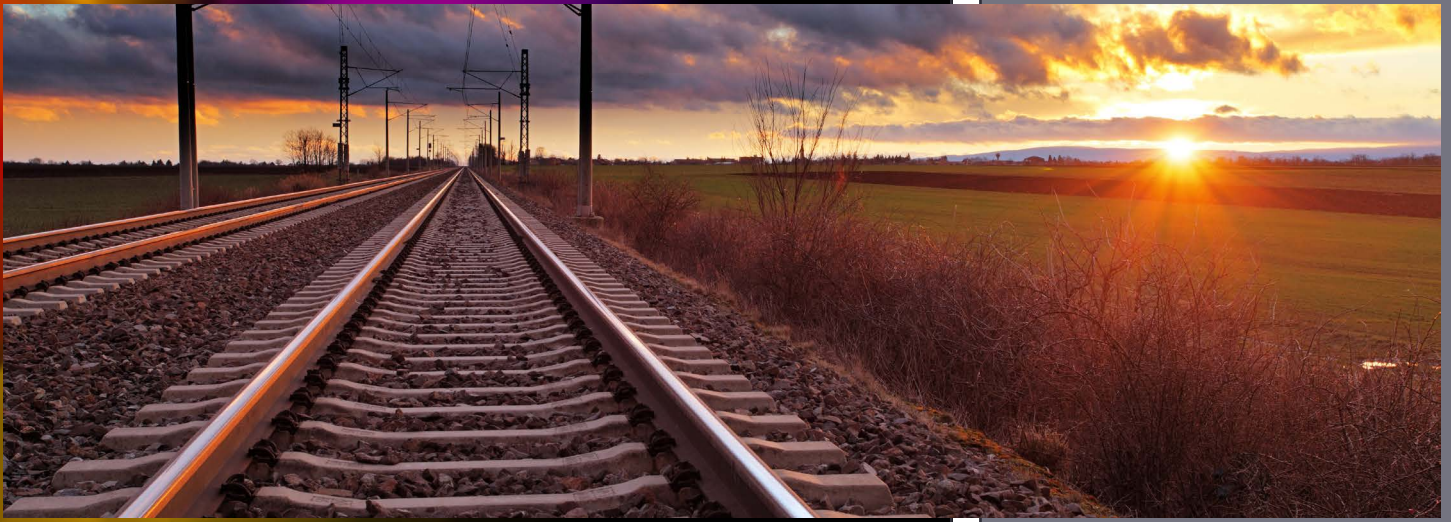
- Put a different lens on the 'robust assessment of principal risks' in Provision 28. This is no longer being done purely

from an external reporting or compliance perspective but as a vital starting point to ensure that the board's activities under Provision 29 have the right foundation or basis. Firstly, that the principal risks identified are truly relevant to the 'sustainable existence' of the company (its business model, performance, solvency, liquidity and reputation); secondly, that they are being assessed (and described) at an appropriately granular and specific level, and thirdly, that responses (mitigations, controls, etc.) are robust and can be relied on by the board in making its declaration.

- Refocus management teams on whether the design of controls is fit for purpose in light of changes within the company and in its external environment, rather than just whether controls were operating.
- Create formalisation and new disciplines, for example, via newly established roles and structures, documentation and investment in systems.
- Clarify governance arrangements with respect to risk management and internal control.
- Refine monitoring and review processes at management and board level to provide ongoing assurance and drive improvements.
- Re-evaluate the sources of confidence or assurance that boards rely on to make their public declarations.

Whilst those engaging directly with us and other risk and governance experts may represent a self-selecting group, this broader trend is undeniable. Our review of over 150 FTSE annual reports and accounts (ARA) with December 2024-March 2025 year ends also reveals a consistent theme – companies are taking Provision 29 seriously.¹

1. References to any company in this report are based on public disclosures made within its latest ARA available as at 30 June 2025.



We have heard that some companies may be reluctant to disclose enhancements to their risk management or internal control frameworks, or to significantly revise their articulation of principal risks, for fear of potential jeopardy. But that fear is misplaced. The FRC revised Provision 29 of the Code precisely to encourage progress, support thoughtful change, and promote responsible risk-taking. Continuous improvement efforts should be a point of pride – not hesitation. Companies should feel confident in reflecting these developments in their annual reports. This aligns with the spirit of "comply and explain" and reflects what the FRC intended when issuing the 2024 Code.

Richard Moriarty
Chief Executive Officer, Financial Reporting Council

However, disclosures are not always fully reflective of companies' efforts. This is why our findings and recommendations are based on a combination of insights from public disclosures in ARAs and anonymised insights from our extensive engagement.

As with most regulatory changes, FTSE 100 companies have taken the lead – their thinking and preparation are more advanced. With about 18 months until December 2026 reporters make their first declarations, we hope that our insights can be used by all those in scope to benchmark and analyse where they are and to accelerate their progress if needed. Even those who are advanced in their approach will need to remain alert and agile – risks are dynamic, particularly in the current macroeconomic and political context. Therefore, frameworks and material controls will need to be revisited.

Our publication has been written to easily aid such analysis:

- [Section 2](#) sets out the activities companies had been carrying out in 2024 to plan and prepare for Provision 29.

- [Section 3](#) discusses what companies had been doing to revisit and refine the foundational arrangements supporting the material controls declaration.
- [Section 4](#) addresses focus areas for 2025.
- [Section 5](#) covers our recommendations on how to create a cohesive and compelling narrative across the ARA, such that readers are clear and confident on how companies manage enterprise and disclosure risk.

The FRC repeatedly emphasised a proportionate and bespoke approach to implementation – and from our work this really seems to have landed. What remains to be seen is whether the varying approaches to implementation due to the absence of a prescribed framework, mandatory external assurance requirements or direct regulatory oversight will deliver cost of capital benefits in the long term.

Authors



Mala Shah-Coulon
Associate Partner
Governance and Public Policy
+44 20 7951 0355
mshahcoulon@uk.ey.com



Maria Kepa
Director
Governance and Public Policy
+44 7795 645 183
mkepa@uk.ey.com

We dedicate this report to **Ken Williamson**.
We also thank Luke Benson, Kavita Behera and Hriday Verma.

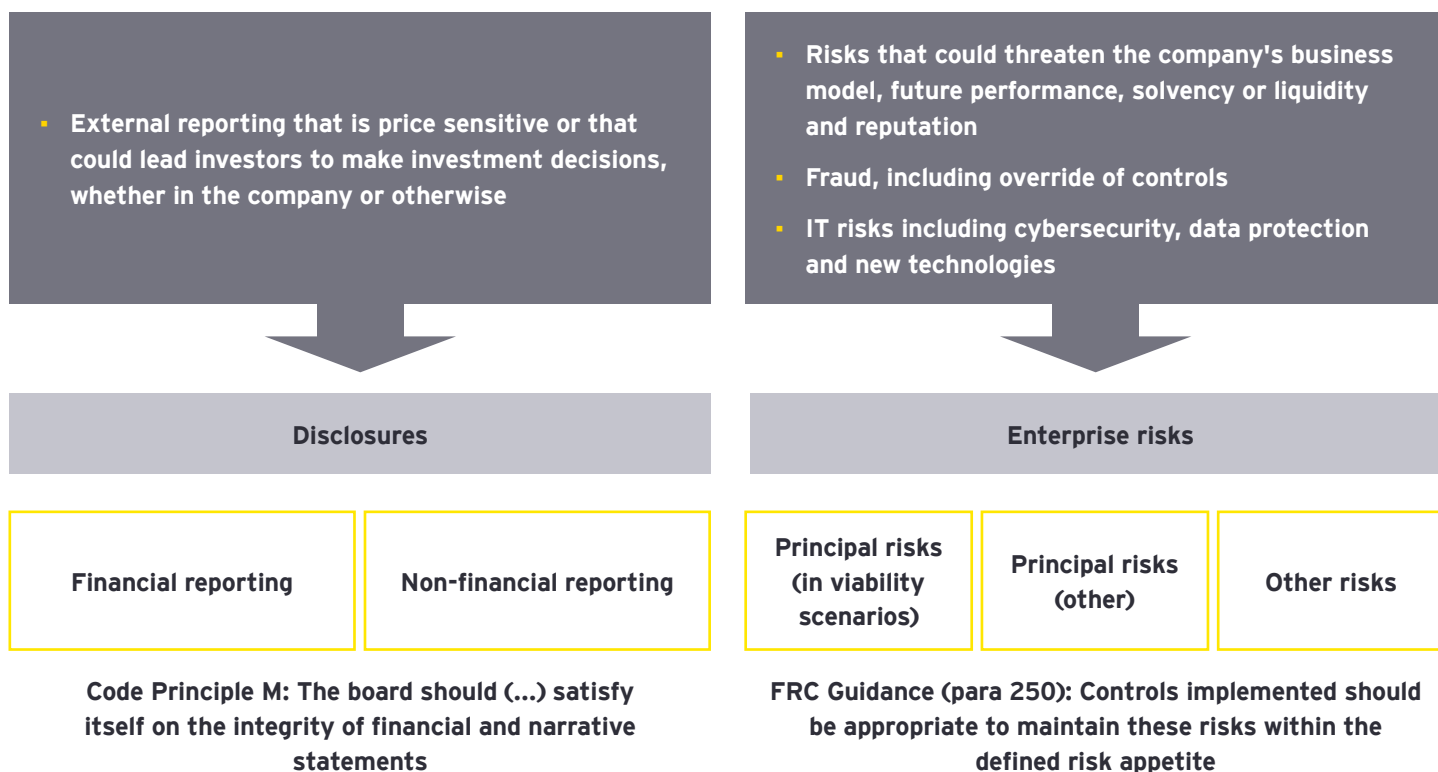
2. Steps companies were taking in 2024

The insight companies voluntarily provided in their ARAs about the activities to prepare for Provision 29 varied greatly. Some, like [Endeavour Mining \(Figure 1\)](#), included detailed callouts. Others did not go much beyond acknowledging that the Code was changing. In this chapter, we have synthesised themes evident in the reporting that resonated with our individual engagements.

2.1. Common understanding

There is general consensus that material controls need to address both disclosure risks and enterprise risks.

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





In respect of disclosure risks, there is now increased recognition that these should not be limited to disclosures within the ARA. Preliminary announcements, other regulatory news announcements and even investor presentations can, in fact, be more price-sensitive. Standalone sustainability reports or other non-financial reports may also require consideration.

In respect of enterprise risks, companies used this as an opportunity to revisit the risk management process rather than focusing only on risk responses and their monitoring. There has also been growing acknowledgement that some principal risks are outside of a company's control; therefore, whilst there may be some mitigating responses, they are unlikely to qualify as controls. This distinction is important as not every response can be meaningfully assessed for operational effectiveness. Business continuity, disaster recovery, or crisis response plans might be in place, but their effectiveness, or otherwise, may only become apparent when they are deployed.

2.2. Planning for Provision 29 compliance

Organisations rightly approached planning for Provision 29 compliance with the intention of leveraging existing risk management mechanisms. [Rio Tinto](#) summed it up well, stating that it aims to achieve a proportionate and practical response to the new declaration, which complements its existing SOx programme. In a similar vein, [BP](#) referenced deploying its existing processes to meet the new requirements, adding elements where appropriate whilst avoiding duplication and minimising extra work.

To enable this, companies needed to clarify their governance arrangements, establish management teams and develop implementation plans that reflected the maturity of their risk management and internal controls.

2.2.1. Clarifying governance arrangements

According to the Three Lines Model, the governing body is not involved in everyday risk management.² Rather, it needs to be actively engaged in its oversight and provide top-down input into its components. To do so, responsibilities should be appropriately allocated between the board and its committees.

Traditionally, audit committees have been concerned with the oversight of risks related to financial reporting and the internal controls over financial reporting (ICFR) associated with it. Today, however, their role is extensive, with most taking on a role more significant than that played by other board committees. So much so that many audit committees have re-labelled themselves as 'audit and risk committees'. Nevertheless, if the audit committee takes on oversight of too many risks beyond those directly related to reporting, it may struggle to adequately discharge its other core duties.

For this reason, oversight of some risks may be delegated by the board to other committees. Even in those situations, the audit committee will typically act as the integrator of most, if not all, risks. This reflects the fact that all principal risks can potentially impact the financial results and the viability of the business. This also aligns with the role the audit committee plays in relation to internal audit and assurance more broadly.

Therefore, it is not surprising that audit committees are overwhelmingly leading in the oversight to prepare for Provision 29. This has led some to redefine their remit and update their terms of reference. For example, the responsibilities of the [HSBC](#) Group Audit Committee were extended to all internal controls and (once defined) all material controls. The Audit Committee of [BAE Systems](#) was renamed the Audit and Risk Committee. The [EnQuest](#) Sustainability Committee was renamed the Sustainability and Risk Committee in 2024. The Committee reviews material controls and held a joint discussion with the Audit Committee in 2024 to review the oversight of risk so that it was appropriately managed.

2. The IIA's Three Lines Model: An update of the Three Lines of Defence, The Institute of Internal Auditors, 2020.

Within financial services, discussions about the clarification of roles between the audit committee and the risk committee were ongoing, with similar conversations in businesses that have a standalone board-level committee overseeing workforce health and safety. Interestingly, the same was less prevalent concerning the roles of board-level sustainability committees, presumably because the remit boundaries and interconnectivity had been agreed in the not-too-distant past, especially by reference to the need for accuracy in Taskforce on Climate-related Financial Disclosures (TCFD) reporting, and environmental, social and governance (ESG) metrics more broadly.

Recommendation

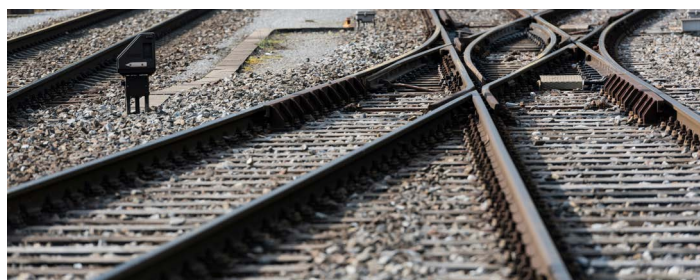
When finalising how directors conduct their monitoring and review, consider any disconnect between the allocation of risk oversight and internal control oversight, avoid duplication or, conversely, matters falling through the cracks.

2.2.2. Setting up the management team

Whilst it is most commonly the audit committee leading the charge on the board's behalf, there is much less consistency in how management teams have been structured. Many companies, such as [Centrica](#), have disclosed that a Management Steering Committee has been established. Some provided more information; [Ocado](#) explained that its team is cross-functional, and [BAE Systems](#) additionally referenced multiple workstreams.

As part of our programme to implement Provision 29, we created a controls sub-committee. This is chaired by our finance director and brings together a number of senior stakeholders in our business, e.g. all our finance heads in our business units. It is therefore wider than our Executive Committee. One of its key roles is to monitor, via an attestation process, compliance against controls in our Group manual. It will meet on a six-monthly basis, and this drumbeat allows a focus on taking remedial action in the highest-risk areas, as identified, for example, from external and internal audits. It reports progress to the Executive Committee and the Audit Committee. This setup also allows us to keep things contained and manageable for the audit committee – for example, it negates the need for a fifth meeting to be added to the Audit Committee's schedule.

Company secretary, FTSE 250



Based on our conversations and those disclosures that provide more detail, teams are often led from within the second line. At [Breedon](#), the second-line Group Risk and Controls team leads the preparation for changes to the Code. At [Vistry](#), this is the role of the Internal Audit and Risk Director. Internal audit is also often involved, especially in the earlier stages of the project, usually leading the mapping of controls to risks and sources of confidence.

Companies have also been recruiting risk and control specialists to lead the preparations. [Spectris](#) recruited a Head of Risk, [Hunting \(Figure 2\)](#), a Group Internal Control Manager; [Bakkavor](#) appointed a Head of Risk and Control – Finance Transformation as well as a Head of Internal Controls and Risk. [Trustpilot \(Figure 3\)](#) welcomed a new Head of Enterprise Risk to join the business in H1 2024.

Recommendation

Preparing for Provision 29 compliance is unlikely to be a side-of-desk job. The board needs to be assured that sufficient resources are in place to make the declaration.

2.2.3. Developing road maps and implementation plans

In 2024, many companies, such as [Croda](#) and [Genuit](#), developed high-level road maps for compliance. Others agreed to more granular implementation plans. For example, [Howden \(Figure 4\)](#) comprehensively mentioned a two-year readiness project focused on Provision 29, whilst [Hunting \(Figure 2\)](#) provided a roadmap of activities related to compliance with all the changes to the Code. Many companies, such as [Legal & General](#) and [Hilton Food Group](#), conducted a gap analysis to determine the next steps in their compliance journey.

Recommendation

As referenced later in [3.4](#), whilst plans are important, they need to have sufficient agility built into them to deal with the dynamic nature of risk.

2.3. Revisiting principal risks

As they are board-approved, principal risks are the natural starting point for enterprise risks that should be addressed through material controls.

Given that risks are dynamic and changing, they need to be reassessed on an ongoing basis within the first and second lines. The outcomes of such bottom-up risk assessments need to be overlaid with a top-down view and challenge from the executive and board, considering the company's strategic objectives and external market factors. This is congruent with the requirement in Provision 28 for the board to annually carry out a robust assessment of the company's emerging and principal risks.

However, conversations with those within risk functions and with board members, indicate that Provision 29 has reinvigorated this reassessment, with new questions and different challenges being raised.

Above all, this needs to be a conversation that contributes to – and is engaging for – executive and board governance and which builds on the progress over the past 25 years rather than attempting a new direction. Concepts like principal risks are well-established, but this process is a helpful nudge to review them and reconfirm their clarity, importance and relevance as the basis for a review of internal control and risk management by the board.

Head of Risk and Assurance, FTSE100

2.3.1. Risk appetite and risk tolerance

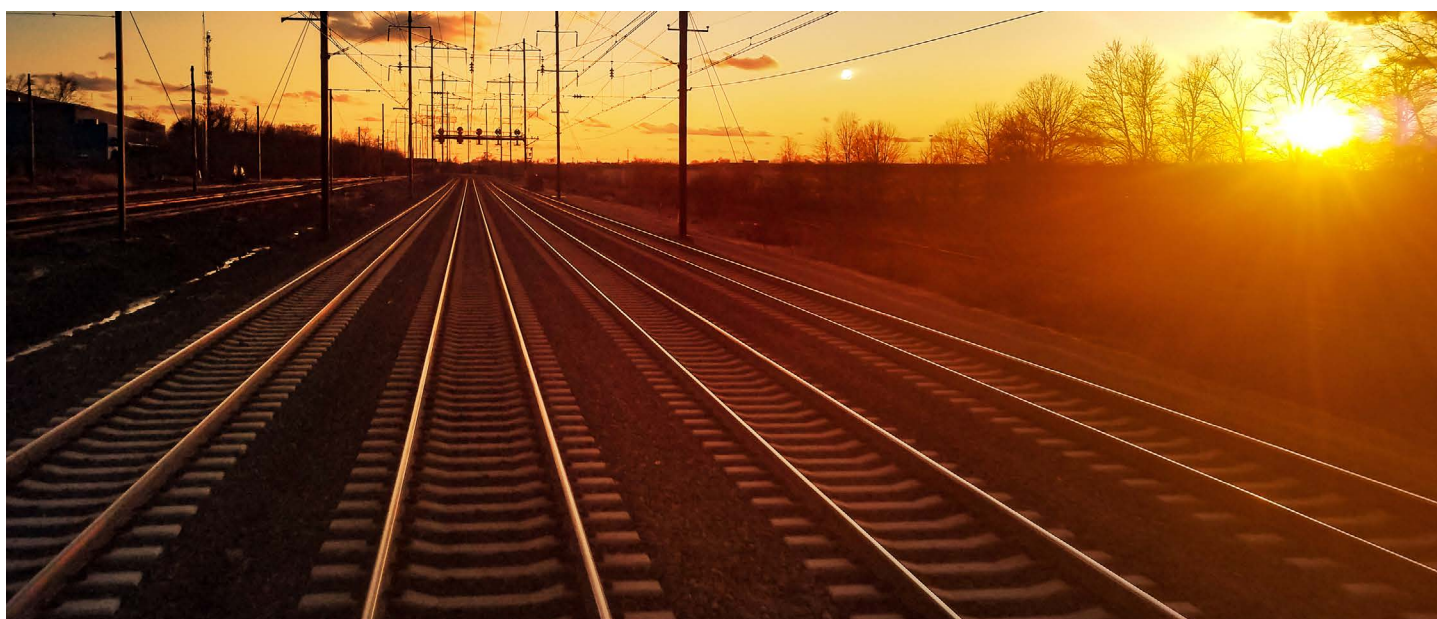
Principle O: The board should establish and maintain an effective risk management and internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives.

241: The board should ensure that the risk appetite is:

- Appropriately defined and articulated
- Aligned with strategy and embedded at various levels of decision-making
- Regularly reviewed and evaluated, and
- Communicated at the appropriate levels throughout the company in a timely manner, including any changes to it

250: (...) Controls implemented should be appropriate to maintain these risks within the defined risk appetite. (...)

Risk appetite must evolve in response to changing internal and external factors (e.g. market conditions, regulatory changes, or organisational priorities). Static risk appetite statements can quickly become outdated. High levels of uncertainty require boards to reassess their risk appetite more frequently to ensure it remains appropriate.



Whilst Principle O requires boards to determine risk appetite, there is no corresponding provision mandating its disclosure. Only around a third of companies set this out voluntarily, as many see risk appetite to be a confidential element of the company’s competitive advantage.

It is, therefore, not surprising that, despite the overwhelming geopolitical volatility, explicit references to revisiting risk appetite, as made by [Howden \(Figure 4\)](#), were rare. However, our engagement indicates that there was more boardroom discussion around this topic in 2024, triggered at least in part by Provision 29 considerations.

When discussing material controls, board members wanted to understand the precision of statements such as ‘the company had operated within its risk appetite’. For many risks, translating appetite into terms that are measurable may not be possible, whereas qualitative statements are hard to operationalise and monitor. Discussions also focused on the distinction between risk appetite and risk tolerance and how the latter might need to be considered when determining the levels of confidence the board might require to sign off on the declaration.

2.3.2. Identifying and evaluating risks

Principal risks are constructed by aggregating risks lower down in the risk taxonomy to create a streamlined, board-level perspective for decision-making. Groupings are typically done by shared causes or by impacts and require balancing actionable granularity with strategic focus.

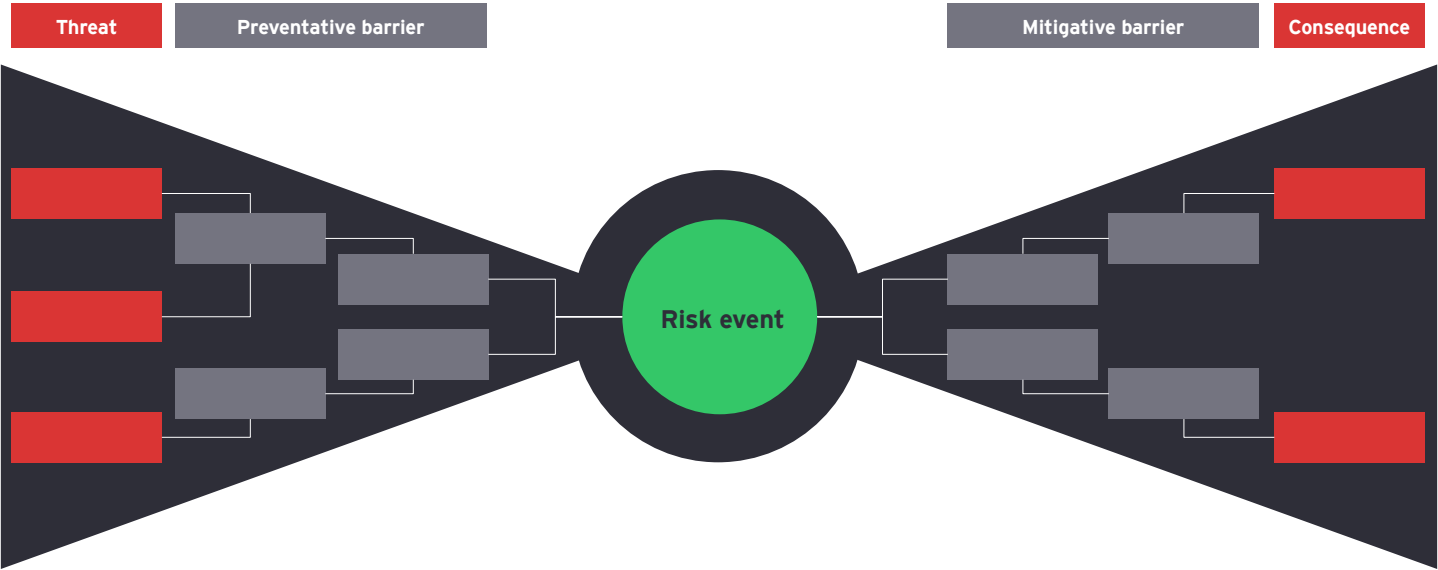
Provision 28: The board should carry out a robust assessment of the company’s emerging and principal risks*. The board should confirm in the annual report that it has completed this assessment, including a description of its principal risks, and an explanation of how these are being managed or mitigated. The board should explain what procedures are in place to identify and manage emerging risks.

247: Risk assessment is a dynamic and continuous process. The nature of risk, including its impact and likelihood, evolves constantly and sometimes rapidly. Risks should be regularly assessed and evaluated. Risk registers may be a useful tool to record and monitor risks; however, they need to be regularly reviewed and updated to reflect any changes.

2.3.2.1. Risk identification workshops

It was quite common for companies to hold internal workshops with risk and control owners, as disclosed by [Keller, IP Group](#) and [Endeavour Mining \(Figure 1\)](#). From speaking with companies, we understand that these often involved completing risk bow ties, as disclosed by [United Utilities](#), testing whether aggregated principal risks capture the most critical threats, and validating principal risks against historical data or incidents (and vice versa).

Risk bow tie



*Principal risks should include, but are not necessarily limited to, those that could result in events or circumstances that might threaten the company’s business model, future performance, solvency or liquidity and reputation. In deciding which risks are principal risks, companies should consider the potential impact and probability of the related events or circumstances and the timescale over which they may occur.

- At [Premier Foods \(Figure 5\)](#), each member of the Executive Leadership Team held an extended workshop with their respective functional leadership teams to consider the full population of risks relevant to their areas of responsibility and the company as a whole. In addition, an extended workshop was held with the non-executive directors to share the enhanced process being used by the Group and obtain their input, given their broad experience. The combined output was then reviewed by the whole Board. This resulted in updates to several principal risks. [Hunting \(Figure 2\)](#) introduced new risk identification processes, with directors completing a risk workshop to agree the strategic and principal risks facing the Group, by reference to its 2030 strategy.
- [SSE](#) changed its method for assessing principal risks to enable more risk-based discussions across the oversight committees and Senior Management. This involved dedicated risk workshops and one-to-one stakeholder interviews.
- [IHG](#) undertook a survey, gathering senior leader opinions on changes in trends and the velocity of principal risks, as well as deep-dive discussions of each principal risk with nominated Executive Committee sponsors.

In addition to the above, significant effort was invested in updating risk registers, including checking completeness back to principal risks. [Trustpilot \(Figure 3\)](#) conducted a full review of its functional risk registers, revising their structure and hierarchy to better align with the organisational structure, with corresponding revision of the roles and responsibilities of the reporting lines. This was used as an opportunity to reaffirm accountability of the first line for management of risk.

The distancing of control understanding and accountability from those in the first line is a learning from SOx that we should pay heed to.

Head of Risk and Assurance, FTSE100

2.3.2.2. Principal risk articulation

Outcomes of risk workshops, revisiting the adequacy of risk responses in the context of risk appetite and attempting to map material controls to principal risks stimulated conversations about principal risk articulation. For example, following the implementation of a new risk framework and oversight approach and the implementation of a new

organisational design, [Rolls-Royce \(Figure 6\)](#) increased confidence in the assessment of its risks, with a focus on mitigating actions to get to an agreed target risk level, as well as more transparent reporting. Rolls-Royce also redefined two of its previous principal risks, technology and climate change (now energy transition), to reflect strategy development in these areas.

Most notably, debates focused on the level of aggregation. For example, during 2024, [JTC \(Figure 7\)](#) refined its risk taxonomy to provide a more granular categorisation of risks, which also necessitated an update to risk appetite. [Clarkson](#), on the other hand, commenced a comprehensive review to rationalise the number of risks, among other matters. [Mears](#) downgraded four risks as they are no longer believed to carry a risk level in order to be categorised as a principal.

A number of ARAs started to reference 'material risks' but didn't fully clarify the term. This category could refer to a combination of those principal risks (within a company's control) and disclosure risks (that can result in errors in external financial or non-financial reporting that are material to investors' decision-making). Equally, it could refer to risks a level or two lower than principal risks in the risk taxonomy.

Recommendation

New terms need to be introduced carefully to avoid creating confusion both within the organisation and at the board level. Principal risks are subject to an annual board assessment process and should be well understood within organisations – they are the natural starting point for attributing material controls. They are likely to resonate better with the audit committee.

Before deciding to attribute material controls to risks lower in the taxonomy, consider whether some principal risks might need to be disaggregated. If material controls cannot be mapped to principal risks, this may indicate that principal risks as disclosed are purely a reporting construct rather than being embedded within the organisation or decision-useful.

This could also be a great opportunity to do some spring-cleaning – maybe some no longer meet the principal risk threshold and should be downgraded, for example, those not reflected in viability statement scenarios and/or those that had been added in response to external expectations as opposed to an internal acknowledgement of the magnitude of the risk.

2.3.3. Other considerations

Some companies, like [LSEG](#), took steps to increase risk awareness or conducted new risk culture surveys to assess the strength of its risk framework. To achieve greater risk identification and assessment, [Johnson Matthey](#) began leveraging a broader network across the business through regular engagement and providing guidance, training and tools. [Rolls-Royce \(Figure 6\)](#) now conducts an annual risk maturity assessment and has put in place risk toolkits that include guidance, templates, tools and training to support the risk management process.



2.4. Identifying material controls

Even directors of organisations with the most mature risk management and internal control frameworks recognised they needed to reassess their considerations in light of the new declaration. This is because, even though the term has existed in various iterations of the Code, governance practices focus on the effectiveness of the overall system of risk management and internal control rather than on the effectiveness of individual material controls that form part of it. As such, efforts to date have focused most notably on identifying material controls.

2.4.1. Material control definition

Definitions create a shared foundation for understanding and a framework for addressing matters systematically. This, in turn, ensures that everyone interprets terms in the same way, reducing scope for confusion.

When the Code was published in January 2024, the lack of an explicit definition of material controls concerned many organisations about the risk of inconsistent interpretations across the FTSE. The FRC, however, reiterated on multiple occasions that it is for a board to determine what should comprise its material internal controls.³

This encouraged companies to dedicate time in 2024 to creating their own definition of what a material control is in the context of their business and organisation. However, the typical approach of a definition that narrows down from an existing broader concept often proved to be of little use, as companies realised that material controls are not necessarily a subset from within the population of already identified controls.

As a result, some companies have chosen not to define material controls at all, or propose definitions that are principle-based. Points considered often included:

- **Significance to achieving organisational objectives** – this allows material controls to include activities beyond those more traditionally associated with control, such as executive committees, risk forums, cultural factors, or decision-making frameworks.
- **Materiality thresholds that are not defined purely by reference to financial materiality** – rather than attempting to create a uniform materiality threshold, these may need to be defined specifically for individual risks -10% customer churn, 20% employee turnover, 5% drop in share price, financial reporting error in excess of 10% of profit before tax. Any such thresholds are at the company's discretion.



- **Preventing not just downside risk from occurring but also opportunities from being missed** – this links material controls to the concepts of risk appetite and risk tolerance. If directors' attention is over-indexed on preventing downside risk, inadvertently, companies may end up operating below their stated risk appetite.

In this context, an effective definition becomes less of a filter to discern material controls and more of a sense check of whether a set of activities proposed as a material control does, in fact, play that role within the organisation's risk management and internal control framework. This approach is also more conducive to recognising that gaps might exist and new material controls may need to be established. For example, [Keller](#) referenced a new project performance management standard that will be rolled out through the Group and become a material control in 2025, mitigating the principal risk of ineffective management of their projects.

Project management controls through the new PPM standard

The new Project Performance Management (PPM) standard and supporting guidance is planned to be finalised by Q1 2025 and then rolled out to the Group throughout 2025. The standard will be operationalised through a PPM application, with approval workflows configured in line with Board-delegated authorities. Furthermore, training on PPM will be delivered to all impacted employees. PPM is a material control for one of our principal risks – the ineffective management of our project. This material control will need to operate by 2026 to effectively mitigate the risk. These controls will be implemented along with the implementation of the standard and application, and tested throughout 2025 by the second-line assurance team.

[Keller Group 2024 Annual Report, page 125](#)

Although many companies have now defined material controls, and some, like [Breedon](#) and [Weir](#), confirm this in their annual reports, very few have made that definition public, and we don't expect many more will. One exception is [Derwent \(Figure 8\)](#), which states: *We have defined our material controls as those that are most important in mitigating key risks that threaten the long-term sustainability of the business, and where a failure of their effective operation, or a resulting omission and/or misstatement of information caused by the control failure is likely to influence decisions made by users of the information.*

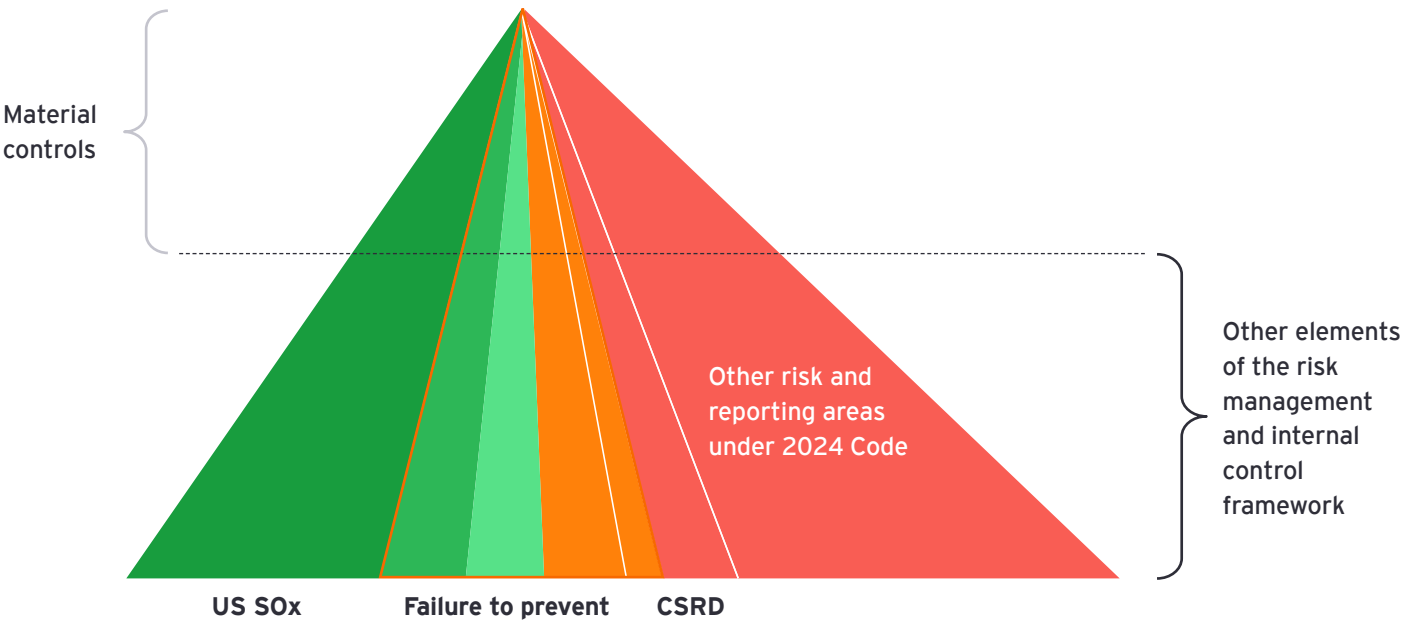
Our engagement with companies indicates that definitions most commonly reference material controls as:

- Being the most critical, important or significant controls
- Those that would have the most influence in mitigating or reducing the impact of a risk
- Safeguarding the interests of key stakeholders and the license to operate
- Controls whose failure could lead to:
 - A material impact arising from the realisation of a principal risk
 - Material misstatement of significant financial or non-financial reporting
- Those whose owners are senior leaders within the business

We recommend that any definition needs to be precise enough to be operationalised.

2.4.2. The ‘top-slice’ approach to identifying material controls

When the Code was published, there was immediate agreement about the need to leverage existing programmes and initiatives to the extent possible. Companies focused on identifying their key controls and designating the top slice as material controls.

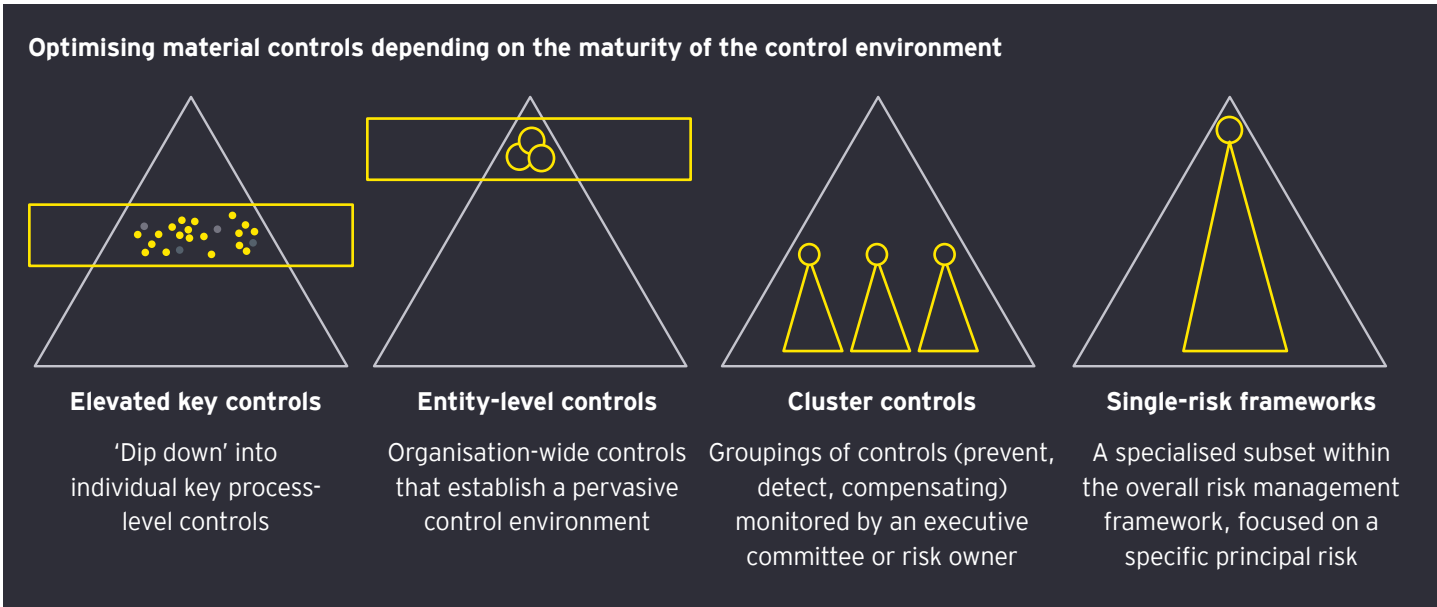


However, when presented with this subset of key controls, audit committees raised concerns. First, the number was too high for them to effectively oversee. Second, the approach failed to demonstrate how the entire principal risk was being addressed. Many teams were asked to come back with a refined proposal.

2.4.3. The ‘pick-and-mix’ approach to identifying material controls

These challenges led to an increased focus on leveraging the maturity of an organisation’s control environment to achieve both a reduction in the number of material controls and appropriate risk coverage.

Companies moved to consider a combination of four main types of material controls. The choice within this pick-and-mix approach is predicated on whether the maturity of the environment is sufficient to provide confidence in the effectiveness of a material control’s operation.





2.4.3.1. Entity-level controls

These are organisation-wide controls that establish a pervasive control environment, setting the tone at the top through leadership, governance and ethical guidelines.⁴ They include policies, risk assessment processes, monitoring mechanisms and communication systems that influence the entire internal control framework and are not confined to a divisional or regional level.

From our conversations, entity-level controls most commonly designated as material controls are those related to the code of conduct and whistleblowing or speak up activities.

In 2024, many companies chose to comprehensively revisit all their entity-level controls. For example:

- [Genuit](#) is performing a full review of its entity-level controls, with the objective of consolidating existing controls and identifying potential areas of improvement.
- [Drax \(Figure 9\)](#) is formalising its library of entity-level controls.

- [JD Sports Fashion \(Figure 10\)](#) continued its work to refine and assess the design of entity-level controls, focusing on alignment with the COSO framework and ensuring these controls effectively support governance and risk management objectives. Action plans were put in place to strengthen areas identified for improvement, and progress is being closely monitored by the Executive Risk Committee. The assessment of entity-level control operational effectiveness will form part of the Group's ongoing Provision 29 compliance efforts.

Undertaking such reassessments is valuable, as not every entity-level control can be meaningfully designated as a material control or subsequently assessed for effectiveness.

In some cases, more formalised documentation is necessary. Below is an illustrative example of a code of conduct-related material entity-level control set out by reference to multiple control areas of the COSO framework:

Activity	Element	COSO area of control	Steps
Maintain an up-to-date and relevant code of conduct	Documented policy	Control environment or risk assessment	<ul style="list-style-type: none">▪ Create a written code of conduct that addresses risks particular to the organisation and outlines expected behaviours.▪ Perform periodic reviews to ensure the code remains relevant in light of the evolution of the business, new risks and regulatory changes.
Ensure the workforce is aware of the code and understands it	Communication and training	Information and communication	<ul style="list-style-type: none">▪ Regular training programmes ensure that the workforce understands the code and its application.▪ Senior management and the board visibly endorse and model the code, reinforcing its importance (e.g. through public statements).
Monitor adherence to the code	Enforcement mechanisms	Control and monitoring activities	<ul style="list-style-type: none">▪ Monitoring of training completion.▪ Timely investigations, and disciplinary actions for violations.

4. Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control – Integrated Framework definition: Entity-level controls are controls that operate at the organisation-wide level to establish the tone, culture, and processes that support the internal control system, including governance, risk management, and oversight activities. Whilst other definitions exist, these are not UK-specific.



2.4.3.2. Single-risk frameworks as material controls

A single-risk framework functions as a specialised subset within the overall risk management framework, focused on a specific principal risk. It operates under the governance structure of the overall framework, adhering to its risk appetite, three lines model and reporting lines. It uses the same methodologies (e.g. risk assessment scales, likelihood-impact matrices) to ensure compatibility, and will often include one or more entity-level controls or their elements. A single-risk framework can be localised to the needs of a particular country or business unit.

‘Health and safety’ is a common example of a single-risk framework, as illustrated by [Barclays \(Figure 11\)](#). Many organisations designate their Sarbanes-Oxley Act (SOx) controls programme as a single material control.

Individual key controls are unlikely to exert influence over a principal risk unless they are individually significant and can lead to an increased risk of a weakness in a material control. It can, therefore, be preferable to consider a framework of controls to be the material control.

This includes activities across the first, second and third lines relevant to that particular risk, conducted by in accordance to related policies and procedures that are regularly reviewed and updated to reflect changes in the business and its environment.

Group Audit Director, FTSE 100



2.4.3.3. Cluster controls

Single-risk frameworks are the most comprehensive way to evidence that a risk is being managed. Where the maturity of such a framework is insufficient to conclude on its effectiveness, some organisations group prevent, detect and compensating controls related to a narrower risk area, designating this cluster of controls as a material control. The combined effectiveness of the controls will be monitored by a risk owner such as an individual, an executive risk committee or a regional or divisional forum that oversees key risk indicators, results of control assurance and others. This oversight mechanism is referred to by some organisations as a governance control and designated as the material control. However, referring to the entire grouping as a cluster control highlights the dependence of the governance control on the underlying transaction-level controls. This differentiates cluster controls from entity-level controls, which operate top-down.

In some cases, a monitoring mechanism that could be evolved into a cluster control had already been in place; in others, a new one needed to be introduced. In the latter case, companies need to be mindful of proliferating too many new committees and forums.

It is critical that cluster controls are not just a veneer but thoughtfully designed, robust mechanisms with precisely defined and documented activities that can be evidenced and, if needed, tested for operational effectiveness.

Common examples of cluster controls are divisional CFOs responsible for monitoring ICFR in their division or regional security forums overseeing cybersecurity in a particular region. Whilst this is not explicitly called out by [Drax \(Figure 9\)](#) as having been designated as a material control, the description of its risk management committees at the business unit and Group function level reflects how cluster controls can function.

We elevated an existing risk forum to be a material control. What the forum was required to do did not change dramatically, but it was important to raise its awareness that, as a material control, it is now beholden to a higher standard of operation and needs to document its activities in more detail.

Group Head of Risk, FTSE 100



2.4.3.4. 'Dip-down' approach

Where cluster controls are not the right answer, companies dip down to identify key controls within individual processes and elevate those to material control status.

This is not dissimilar to the initial 'top slice' approach and will generally increase the number of material controls and risks leaving gaps. Given their pervasive nature, gaps can be addressed via entity-level controls, provided they have been documented in a manner that sets out how the entity-level control targets those areas.

In some cases where companies have designated a single-risk framework as a material control, they have additionally elevated a key control from within it to material control status. For example, the valuation of a particularly judgmental financial statement line item that is highly price-sensitive to investors might be separated out from within the SOx framework to provide the audit committee with more granular insights on the matter.

Recommendation

Section 414CB(2) of the Companies Act requires companies to describe how the company manages its principal risks. A full mapping of mitigations to principal risks will, therefore, include more than just material controls. As a result, some companies designate elements of process narratives as a material control. For example, some companies describe the process related to annual performance appraisals as a material control for talent risk. With some effort made to explain how the effectiveness of that process is going to be assessed, companies may be able to articulate the related control.

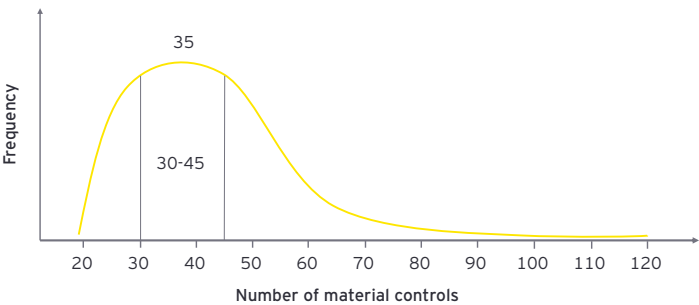
Standard control documentation:

Who	The title or role of the person performing the control
When	Timing of the control being performed
Why	Control objective, linked to the risk it mitigates
What	Description of the control activity, including any triggers for follow up or notification
How	List of documents that evidence the performance of the control



2.5. The magic number

The number of material controls continues to evolve as management teams refine their approach and address challenges from audit committees. The broad range in mid-2025 has settled at between 20 and 120 material controls.

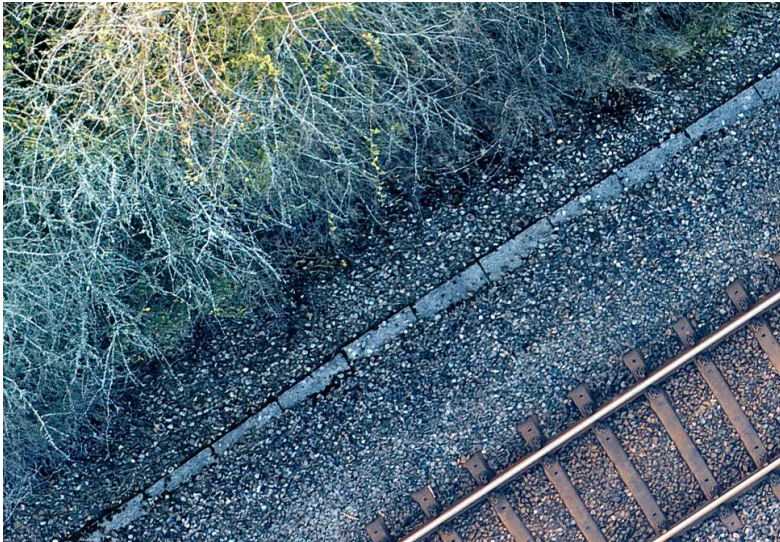


The higher end of this range relates to financial services companies, and particularly banks. These institutions are generally controlled in a very prescribed manner due to intense scrutiny from both UK and international regulators who mandate comprehensive controls to ensure financial stability, consumer protection and market integrity. For example, the Senior Managers and Certification Regime (SM&CR) mandates regular reporting on control effectiveness to regulators to demonstrate accountability. Many institutions have, therefore, chosen to designate existing key controls as material, given their effectiveness is already monitored, reported on to the board, and often scrutinised by the regulator.

Companies at the lower end of the range are typically those that are US SOx compliant or are subject to similar international internal control regimes.

The most common number is circa 35 material controls. This is a preliminary position, and we expect this number may decrease over time as companies mature their control environment.

As we had anticipated, unless companies have a single material control over financial reporting, material ICFR makes up around a quarter of the entire population, often including topic areas such as segregation of duties, balance sheet reviews, goodwill and other impairment considerations, going concern, tax and treasury. Matters such as budgeting and investment approvals are often designated as financial controls rather than ICFR.



In March 2021, the Prudential Regulation Authority (PRA) published Policy Statement PS6/21 (“Operational resilience: Impact tolerances for important business services”), alongside the Financial Conduct Authority’s (FCA) equivalent PS21/3 (“Building operational resilience”), confirming new rules to strengthen the operational resilience of banks, insurers and other in-scope firms.

Embedding operational resilience into risk management and governance processes involved, amongst others, identifying important business services and setting impact tolerances for their maximum acceptable disruption; mapping processes, systems, and dependencies; as well as commencing a programme of scenario testing and identifying vulnerabilities. It culminated in the compilation of a self-assessment document, reviewed and approved by the board, demonstrating how the operational resilience requirements have been met.

Since 31 March 2025 (the end of a transitional period), firms must remain consistently within their impact tolerance for each important business service in the event of a severe but plausible disruption to their operations. They are expected to maintain operational resilience as a dynamic activity (including regular scenario testing and reviews of, and updates to, the self-assessment document) and continuously invest in and improve their operational resilience frameworks. The PRA and FCA will review firms’ self-assessment documents and examine their compliance as part of routine supervisory engagement or on an events-driven basis.



2.6. Dynamism

Risks are dynamic and, especially in the context of the current volatility, may be elevated to principal risk status at short notice, including close to the year-end.

285: The board's role should be focused on reviewing material controls, as agreed. Risks are dynamic and will change over time, therefore the material controls will need to adapt to such changes.

Reflecting this, [BT \(Figure 12\)](#) categorises its Group risks as either enduring or dynamic, stating that enduring risks need consistent, long-term structures to manage them. Dynamic risks are either point risks that are potentially materially significant at a particular time, and need focused attention as they cannot be managed within its existing control framework or emerging risks that are new and often long-term, with the potential to be materially significant.

It is for this reason that the focus on the average number of material controls should not detract from the fact that this is not a 'one-and-done' issue. In 2024, some, such as [Ocado](#), created an initial internal list of material controls to be refined in the following year. Others concluded that in areas where risks were developing and changing, it was not prudent to commit to defining a material control just yet but rather to maintain a watchful eye and allow for an organic evolution of control activities first.

2.6.1. Material controls in waiting

From our conversations, some companies have identified material controls in waiting. These are controls ready to be elevated to material control status if the risk escalates. Whilst

these are not being monitored in the same way as material controls, they are properly documented with a list of records that can be collected to support their effectiveness, and they have an assigned owner who may be required to complete a self-assessment.

This approach achieves two objectives in tandem. Firstly, it avoids a cliff-edge safeguarding from having to explain in the year-end declaration that the effectiveness of a material control could not be confirmed. This counters potential resistance to elevating a risk to principal risk status because it does not have a material control identified against it. Secondly, it maximises the efficiency of already being out in the business speaking to risk owners.

2.6.2. Temporary material controls

Whilst the declaration of effectiveness is as at the year-end, the board needs to monitor the risk management and internal controls framework throughout the year. Regular risk monitoring may identify the need for material controls to be established at short notice, some of which may cease to be needed at year-end.

Talking to executive leaders about what activities they rely on, and which are material to their ability to sleep soundly at night, can be a provocative and revealing discussion. I am learning that executives are often reliant on highly dynamic controls during the year – for example, targeted steercoos stood up to tackle emerging topics, which could even have fulfilled their purpose by the balance sheet date.

Head of Risk and Assurance, FTSE100

3. Getting the foundations right

By design, material controls reflect a top-down approach. They do, however, require solid bottom-up foundations to achieve their objectives. In 2024, companies were strengthening or refining those foundations in various ways, such as formalising definitions and documentation, redefining boundaries between the three lines, investing in systems to drive greater standardisation across the organisation and introducing or refining control self-assessments. Even companies with a well-structured and defined control environment saw Provision 29 as a catalyst for revisiting their arrangements.

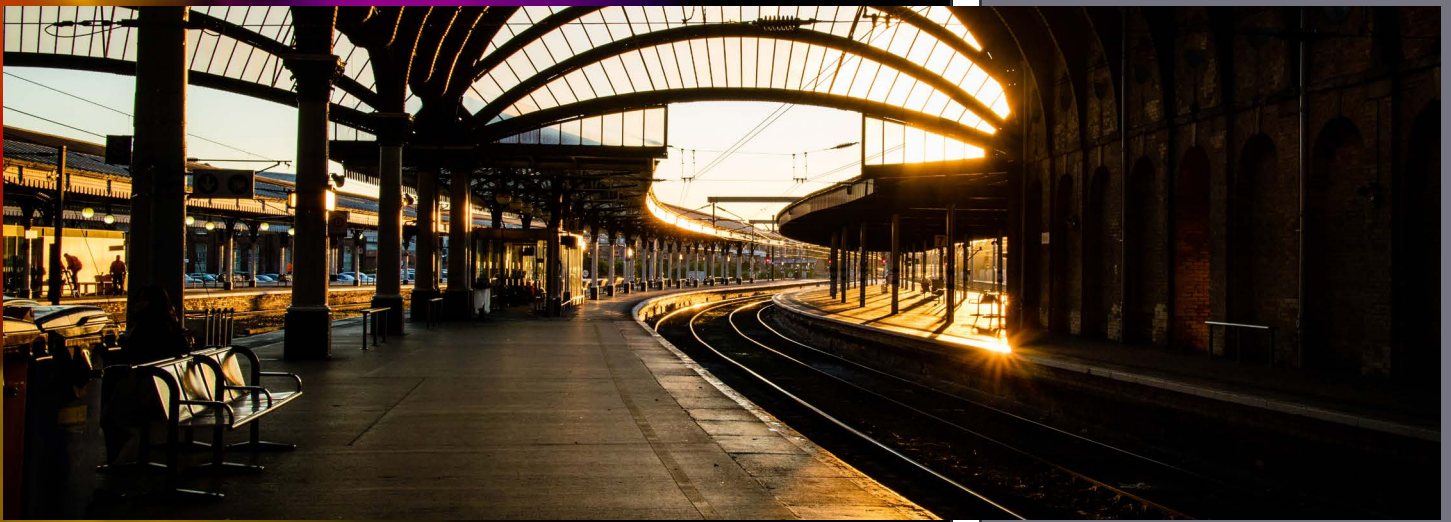
Provision 29 gave us a mandate to clean up and clear out some of the practices that had become outdated and refocus on not just whether controls were operating, but that their design remained fit for purpose in light of changes to risks and changes to our organisation.

**Internal controls change programme director,
FTSE 100**

Several companies commenced holistic review programmes, for example:

- [Balfour Beatty](#)'s programme to implement an enhanced and matured Group-wide Internal Control Framework (ICF) involves a collation of the Group's key controls from various sources across the Group; their validation with key stakeholders, working with subject matter experts to understand control owners, the control design and the verification process; as well as establishing a standardised template for documenting internal controls in the ICF and establishing a tiering system aligned to organisational hierarchy.
- [Howden's \(Figure 4\)](#) Key Controls Project is a wide-reaching improvement programme addressing governance, controls and evidence.
- [Vistry \(Figure 13\)](#) is making improvements to enhance the level of formality in its risk management and control framework, including through the introduction of formal definitions for all operational, financial, IT and people-related controls to achieve standardisation. Additionally, it is investing in a single system to support the automation of controls.
- [Capita](#), in 2023, initiated an internal controls improvement programme to document key business processes and controls to enhance and standardise the company's internal control framework.
- [Bunzl](#) included a non-financial objective related to the delivery of its internal control programme in the CFO's bonus arrangements.

To date, the greatest focus has been on ICFR. Some companies, such as [JD Sports Fashion \(Figure 10\)](#), explicitly state that their internal controls programme has a near-term focus on ICFR and IT controls, with identifying and evaluating material controls over other areas being a future development.



3.1. Financial reporting controls

A natural approach for dual-listed companies like [GSK](#) was to align their approach to material controls over financial reporting with their existing SOx processes.

Many companies that were not subject to US SOx requirements began to consider the need to bolster their ICFR as it was widely anticipated that the outcome of the Government's 2021 consultation [Restoring trust in audit and corporate governance](#) would be scoped around ICFR.

In its 2021 annual report, [Reckitt](#) referenced a multi-year controls transformation programme in preparation for internal controls changes arising from the consultation. It has since been providing regular updates. Alongside meeting the requirements of the Code, the programme aims to embed a control-focused culture that will help strengthen internal controls across the Group.

- In 2022, the Group developed an updated standardised and risk-focused controls framework for financial and IT general controls, and tested it in three pilot markets.
- In 2023, the programme was updated to include new evidence standards to enable consistent documentation of the operating effectiveness of ICFR and IT general controls. Following the launch, the second line of defence team, supported by external advisors, conducted a comprehensive gap assessment to determine the required uplift to comply with the new framework and evidence standards. As anticipated, gaps were identified in relation to the retention of evidence and the formality and consistency of control operations, compared with the framework and standard.
- In 2024, remediation work continued alongside a programme of control testing covering financial and IT general controls.

In its FY24 annual report, [Tesco](#) discussed work being undertaken to enhance the ICFR framework to meet future corporate governance reforms. The framework is underpinned by three pillars: entity-level controls, business process controls and IT general controls. A key financial controls framework is maintained and used as the basis for focused second-line control activities, with greater rigour around controls testing having been implemented. In the FY25 annual report, [Tesco \(Figure 14\)](#) highlighted the strengthening and centralising of the internal financial control environment noting that the programme is now well advanced. During the year, work continued to embed these processes as business as usual. Regular updates about the progress made by management to remediate and improve IT general controls and IT automated controls were provided to the Audit Committee, which noted significant progress.



Case study: UK companies increase the rigour of key controls over financial reporting

In anticipation of corporate reform in the UK, numerous companies proactively invested in establishing robust internal control functions and enhancing their internal controls across key transactional areas, particularly in relation to financial reporting. This shift was largely driven by a critical self-assessment: many organisations recognised that their ICFR were far from mature.

Companies are now diligently documenting their key controls over financial reporting, which typically encompass:

1. A comprehensive financial reporting risk, governance, and assurance framework
2. Systematic maintenance and monitoring of the financial controls system
3. Rigorous monitoring and reporting of financial control deficiencies

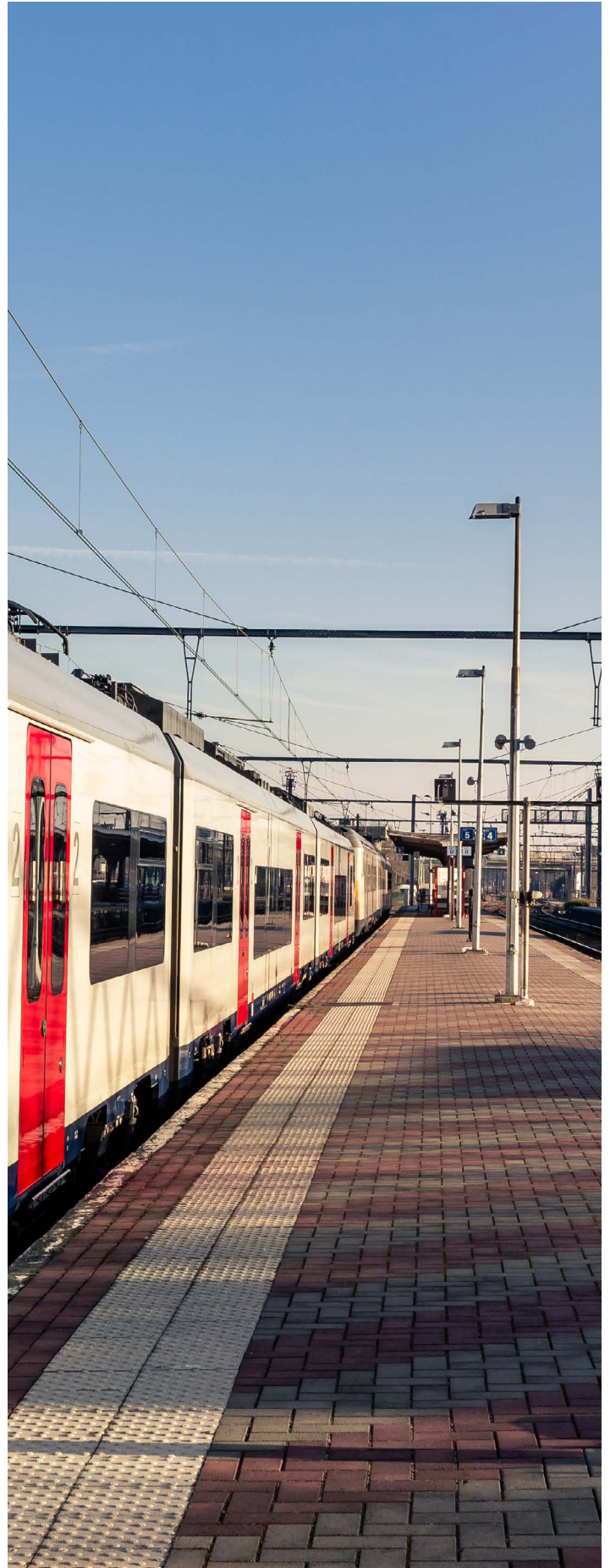
This approach bears a striking resemblance to the controls mandated by Section 302 of the US Sarbanes-Oxley Act (SOx), which addresses disclosure controls supported by Section 404(a) regarding ICFR.

Organisations that have committed to an ICFR programme are now reaping substantial benefits. They are applying a more rigorous lens to their processes and controls, enabling them to identify numerous redundant controls, duplications, and gaps within their operations. Whilst this might be a new undertaking for UK-listed businesses, it would be familiar territory for US-listed companies.

Addressing these issues in a structured manner has not only enhanced their control environments but has also led to increased operational efficiency. For instance, one company I have supported successfully revamped its data governance and strategy, paving the way for more automated controls. This transformation has allowed it to leverage simpler workflows to further automate processes using artificial intelligence.

Moreover, these companies are harnessing the insights gained from their ICFR initiatives and Provision 29 as a catalyst for broader organisational change across their control environments, including automation, cost rationalisation, and standardisation.

Gaston Sanchez-Elguezabal
Partner, Capital Markets
gsanchez-elguezabal@uk.ey.com



3.2. IT general controls

A differential focus on IT controls appears to be a common theme referenced in the above examples. [Hunting \(Figure 2\)](#) also mentions undertaking a review of Group IT controls, and [Informa \(Figure 15\)](#) includes technology controls as a separate element in its diagram illustrating the process of its material controls declaration. [JD Sports Fashion \(Figure 10\)](#) invested in and established a structured remediation programme to drive progress and address key deficiencies in its wider IT general control environment.

Applying a risk-based 'ITGC+' mindset

IT systems and IT controls are foundational to ICFR. However, in line with the requirements of the UK Corporate Governance Code, businesses need to take account of all principal risks, not just financial disclosures. IT system and control scoping should be multidimensional, supporting a broader range of operational risk areas and resilience imperatives. This means a greater number of 'in-scope' IT systems as well as IT controls that expand beyond the traditional.

As an example, I expect to start seeing baseline ITGC+ controls applied to systems that:

- Support critical supply chains
- Hold sensitive intellectual property
- Are critical to business operations
- Process personal data

I also expect to see these controls extend beyond 'change', 'access' and 'operations' – for example, with expanded focus on cyber, data and resilience.

The journey may not be straightforward, but it will enable trust as technology accelerates. An expanded IT control landscape requires a unified approach. The current norm of approaching each risk area in silos will quickly generate inefficiency, duplication and introduce risk. A connected and multidimensional approach to IT risk, on the other hand, will pay dividends in the years to come.

David Lee

Director, Technology Risk

dlee@uk.ey.com

3.3. Non-financial reporting

Although, at least initially, the focus was on ICFR, some companies are now turning their attention to other areas, including non-financial reporting:

- [Mondi](#) acknowledged that non-financial reporting requirements are increasing and that its already robust internal control framework will need to be developed to incorporate such reporting. This has been identified, therefore, as an area of focus from an internal control perspective, and work is already underway in this regard and will continue into 2025.
- [Rolls-Royce \(Figure 6\)](#) is clear that its integrated Group-wide plan for meeting the additional reporting requirements of the 2024 Code addresses principal risks and also incorporates other areas such as financial and non-financial reporting (including sustainability reporting requirements) and compliance.
- In 2024, [BAT](#) launched a cross-functional initiative, which includes representatives from operations, sustainability and enterprise risk management, designed to meet evolving disclosure requirements and ensure assurance on non-financial sustainability-related disclosures. This programme leverages the Group's risk management framework, drawing on its risk management system, methodology and risk registers.
- [RHI Magnesita](#) intends to develop its second-line team to expand its testing scope from key controls over financial reporting to encompass material controls over non-financial reporting.

These are a couple of leading examples, but our conversations indicate that many companies are not well progressed in this area, with non-financial reporting still heavily reliant on spreadsheets and email communications. Now that the prospect of reasonable assurance under the Corporate Sustainability Reporting Directive (CSRD) has been removed, progress may slow down.

3.4. Failure to prevent fraud (FTPF)

Effective from 1 September 2025, large organisations are criminally liable where an employee, agent, subsidiary or other associated persons commits a fraud intending to benefit the organisation (outward fraud), unless it can demonstrate it had reasonable fraud prevention procedures in place.⁵ The [Home Office guidance](#) outlines six principles that those reasonable procedures should be informed by: top-level commitment, risk assessment, proportionate risk-based prevention procedures, due diligence, communication (including training) and monitoring and review.

In essence, the offence is intended to encourage organisations to build an anti-fraud culture, in the same way that failure to prevent bribery legislation has helped reshape corporate culture since its introduction in 2010.

Disclosures within annual reports referenced related preparatory activities. [Vistry \(Figure 13\)](#) mentions a significantly enhanced fraud risk assessment with a new supporting process for identifying, reviewing and reporting both known and potential fraud risks. [Rentokil](#) completed a wider fraud risk assessment, reviewed existing fraud processes, risks and legislation and enhanced its fraud response capability through training and the creation of a dedicated fraud response team. [Bakkavor](#) carried out a fraud risk management assessment to develop an action plan to comply with the expected new legislation in this area.

The positioning of these disclosures alongside those about preparations for Provision 29 suggests that, in many cases, the work is being undertaken cohesively. [Informa \(Figure 15\)](#) makes this point explicitly, noting that it continued to strengthen its Group-wide and divisional controls – in preparation not only for the requirement in the revised Code but also in response to FTPF. [Capita](#) states that its project to implement the ECCTA will support its internal control project aimed at Provision 29 compliance and will also strengthen [Capita's](#) bribery controls. [JD Sports Fashion \(Figure 10\)](#) also makes a similar point.

The Home Office guidance states that 'where the effectiveness of a specific fraud prevention measure is assessed in the declaration made under the UK Corporate Governance Code, it should not be considered necessary to duplicate the work for the purposes of demonstrating that reasonable procedures were in place to prevent that specific fraud.'

In-scope organisations are encouraged to leverage synergies with existing compliance programmes when assessing and implementing reasonable procedures. It is, therefore, both appropriate and pragmatic to dovetail FTPF and Provision 29 preparations and controls.

Ted Rugman
Director, Forensics
trugman@uk.ey.com

However, some of our engagement indicates that this has not always been the case. Unlike [Grafton](#), very few companies identify fraud as a standalone principal risk, as it often cuts across several principal risks. Financial reporting fraud and some instances of greenwashing could be price-sensitive or could lead investors to make investment decisions, whether in the company or otherwise. As such, to avoid duplication, streamline compliance and ensure robust board oversight, the approach to compliance with FTPF and Provision 29 should work bi-directionally:

- Leveraging material controls for FTPF compliance: using existing or enhanced material controls to meet ECCTA's reasonable fraud prevention procedures.
- Leveraging FTPF procedures to strengthen Provision 29: incorporating fraud prevention measures into the broader material control framework.



5. Meeting two of the following criteria: >250 employees, >£36 million turnover, >£18 million assets

Activity	Examples of streamlining reasonable procedures to prevent fraud with the UK Corporate Governance Code requirements
Risk identification and assessment	In the same way that under TCFD, organisations are expected to integrate processes for identifying, assessing and managing climate-related risks into their overall risk management, companies may find it most effective to leverage or incorporate the output of the fraud risk assessment under the scope of FTFPF into their existing risk assessments. Some companies are designating their fraud risk assessment process as a material control.
Entity-level controls	<p>Entity-level controls, such as those related to the code of conduct and whistleblowing arrangements, align with the guidance principle of ‘top-level commitment’ and ‘communication (including training)’.</p> <p>As these entity-level controls will have a much broader impact than outward fraud only, they are already being designated as material controls by many organisations. For example, whistleblowing arrangements can uncover inward and outward fraud as well as other breaches (e.g. health and safety violations and data protection issues).</p> <p>Board monitoring and review of these material controls will, in turn, contribute to demonstrating top-level commitment.</p>
Single-risk frameworks	<p>The fraud prevention framework should be informed by the six principles set out in the guidance and reviewed regularly. As very few companies identify fraud as a standalone principal risk, fraud topics are likely to be covered through activities spanning many risks, for example, data breaches, supply chain risks, anti-bribery or tax evasion, rather than via a single-risk framework material control.</p> <p>It is, therefore, important not to create unnecessary duplication and to document the alignment of fraud prevention with other aspects of the risk and internal control environment, as discussed by IAG (Figure 16). Core to this is streamlining evidence to document reasonable procedures with monitoring and review procedures undertaken for the Provision 29 declaration.</p>
Cluster controls	<p>Formalising cluster controls and reassessing the remit of any existing oversight mechanisms creates an opportunity to consider whether they can play a role in evidencing fraud prevention procedures. Where these are done at a divisional or regional level, this can differentially target those areas where the fraud risk is considered higher, demonstrating proportionality.</p> <p>A procurement oversight committee can monitor controls related to aspects of supply chain risk and also be responsible for overseeing due diligence procedures in conjunction with legal and compliance functions.</p>
Dip-down approach	There is likely to be an overlap between key controls elevated to material controls over financial and non-financial reporting and those related to the risk of fraudulent financial reporting and greenwashing. The interaction with FTFPF might lead to a differential focus on documenting and testing the effectiveness of these controls. This could include monitoring risk indicators that may indicate a potential override of controls or collusion.



3.5. Control self-assessments

Many companies already have a robust process in place for control self-assessments, including a review of the associated attestations:

- [Drax \(Figure 9\)](#) performs self-assessment and review of risk management and internal control activities covering the Group's principal risks. Control owners provide an assessment on the operation of key controls at least twice annually and report on any gaps or control failures identified. These responses are then reviewed by the second-line Group risk team, and the assessments of control operation and effectiveness are periodically challenged and validated to supporting evidence. Additionally, [Drax](#) established a self-assessment of the levels of control and governance that support external compliance obligations.
- [BAT](#) group operating companies and other business units are annually required to complete a controls self-assessment, called Control Navigator, of the key controls that they are expected to have in place. Its purpose is to enable them to self-assess their internal control environment, assist them in identifying any controls that may need strengthening and support them in implementing and monitoring action plans to address control weaknesses. The Control Navigator assessment is reviewed annually to ensure that it remains relevant to the business and covers all applicable key controls.
- [Morgan Sindall](#), as part of the process of identifying material controls, expanded the risk and control matrix used as the basis for the divisional self-assessment process to cover not only financial controls but also operational, commercial, ESG-related and fraud-related controls.
- [Helios](#) implemented monthly compliance control self-assessment declarations provided by each operating company's senior management. These declarations are reviewed by the Group Finance Director, along with any follow-up actions where the Finance team is not satisfied with the quality of the application of the control. A summary is presented to the Audit Committee quarterly.

The above is also borne out in our conversations with companies – many want to empower employees to take ownership of risk management, by enhancing or expanding existing control self-assessments or introducing them, where they didn't already exist:

Control self-assessments are often documented using software – often referred to as Governance, Risk, and Compliance (GRC) tools.

3.6. Implementation of GRC tools

Based on annual report disclosures, many companies, including [Endeavour Mining \(Figure 1\)](#), [Hunting \(Figure 2\)](#), [Howden \(Figure 4\)](#), [JD Sports Fashion \(Figure 10\)](#) and [Vistry \(Figure 13\)](#), moved forward with the implementation of GRC tools.

[Serco](#) noted that a key focus throughout 2024 has been on the design and implementation of the risk management module of its new GRC tool. This module replaces legacy risk register systems to provide increased functionality, transparency and reporting. Its capabilities are being rolled out across the Group. Its implementation is a key enabler for [Serco's](#) work in preparation for the implementation of changes to the Code.

These tools automate risk assessments, control monitoring and compliance reporting and support the evidencing of risk management by providing a centralised platform for risk owners to oversee controls and demonstrate compliance. GRC tools can help reduce manual errors, improve consistency, and provide real-time visibility into control effectiveness. They also automate the process (e.g. sending reminders), enhance accuracy, and centralise data, allowing better monitoring and, in some cases, can be tailored specifically to a particular cluster control.

The introduction of P29 has clearly triggered us to review our existing policies, frameworks and information flows, but this has undoubtedly also come at a cost; for example, we have had significant new hires (internal controls manager, IT manager, etc.) and we have had to implement a GRC tool for documentation and monitoring purposes. It is unlikely we would have done this in the absence of Provision 29.

Company secretary, FTSE 250



3.7. Investment in second-line capabilities

Although many annual reports make reference to a clearly defined three-lines model, responsibilities can easily become blurred when resources are tight and companies are undertaking process and control transformations. In such situations, the first line can lean heavily on the second and third, whether for assurance, consultative support, or just to 'get the job done'. This can be further exacerbated when two or more of the Head of Audit, Head of Risk and Head of Assurance roles converge into one.

Disclosures and conversations indicate that in 2024, organisations of all different sizes were investing in their second-line capabilities, for example:

- The internal risk function of [PageGroup](#), previously combined with Internal Audit, was restructured to better prepare for the reform.
- [JD Sports Fashion \(Figure 10\)](#) is separating the risk management function in line with a traditional three lines of defence model, and an experienced Head of Risk will join the Group.
- [RHI Magnesita](#) established a separate team to perform testing of the key controls over financial reporting, which will be developed to encompass material non-financial controls.
- [Lloyds](#) clarified the roles of risk and control owners, second-line risk specialists and chief control officers across all parts of the business to ensure consistency and enhance focus on controls and expertise.
- [Experian](#)'s risk management programme includes a Second Line of Defence Strategic Plan, which incorporates an annual self-assessment of maturity progress and a rotating external validation, where target maturity is benchmarked across relevant industry peers, including financial services.

- [Johnson Matthey](#), at the end of 2024, decided to separate the Group Risk and Group Assurance functions to provide the Board and Management with independent, risk-based, and objective assurance, advice, insight and foresight. The Group Assurance Director (formerly the Director of Assurance and Risk) will continue to report functionally to the Audit Committee Chair and administratively to the Chief Financial Officer. This positioning provides the organisational authority and status to bring matters directly to Senior Management and escalate matters to the Board, when necessary, without interference, and supports Internal Audit's ability to maintain objectivity.

The Head of Controls is traditionally a role within the finance function focused on ICFR. The 'risk and control mindset' typical of people in this position makes them well-placed to support across a much broader controls agenda. Provision 29, the expansion of reporting requirements related to environmental and social topics, the FTFP offence and programmes seeking to document, standardise and formalise operational controls are just some of the topics being added to their plate.

Companies need to strike the right balance to handle current and emerging demands – choosing between leveraging existing, often siloed compliance and control expertise versus expanding a more centralised cross-functional controls capability. The former can lead to duplication, inefficiency and inconsistency; however, the latter may require organisational and cultural change and risks stretching teams that were originally set up to focus on ICFR too thinly. A happy medium will need to be found. One thing is clear: the role of the Head of Controls is evolving at pace – whilst this poses challenges, it provides a unique and genuine opportunity to add significant value to the organisation.



4. What are companies focusing on in 2025

Companies are at various levels of preparedness. Some, like those referenced in the previous chapter, have made significant strides. Others have not progressed much beyond a high-level gap analysis. This chapter is based on the focus areas disclosed by companies further along on the journey, who will have likely already completed a number of these activities.

4.1. Document and formalise material controls

Companies that identified their material controls and had the list approved (most commonly by the Audit Committee) are now dedicating time to enhancing related documentation. Whilst there is no expectation of rigour equivalent to what is required under US SOx, a degree of formalisation is needed to provide clear criteria for assessing whether or not the control operated effectively.

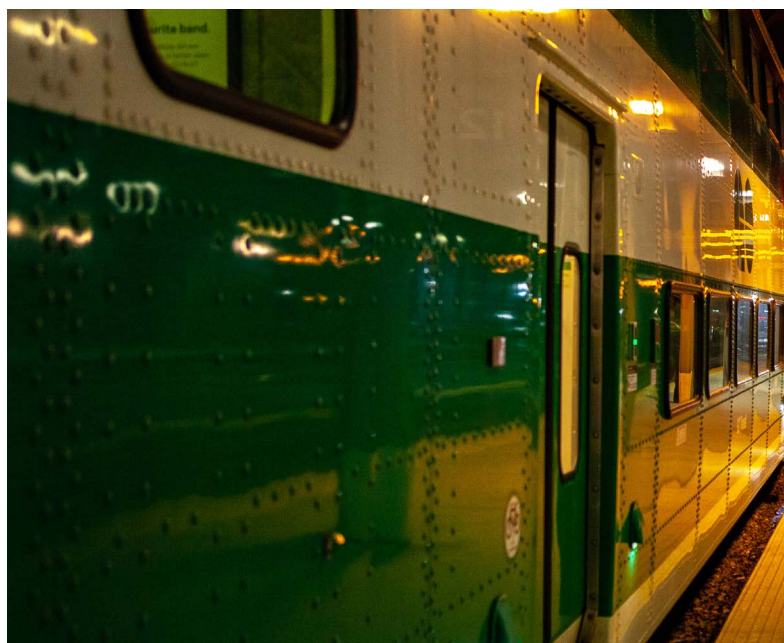
279: The review should consider the risk management and internal control framework of the company as a whole, along with an evaluation of the effectiveness of the processes for ongoing monitoring of the framework. **A set of criteria may be beneficial when conducting a review.** These criteria could examine the effectiveness of the individual controls, the relevance of these controls to the underlying risks and the broader framework itself.

This is especially important for material control categories other than elevated key controls, which are less likely to easily translate into traditional templates for control documentation.

Companies are also formalising what evidence will need to be maintained with respect to material controls and training control owners. Where a GRC tool has been implemented, it is also sometimes being updated for material controls, as noted by [Endeavour Mining \(Figure 1\)](#).

In 2025, we are focusing on embedding the material controls approved by the board last year. This involves meetings with all control performers to ensure that they maintain the appropriate level of evidence to support the planned testing.

Head of Finance Risk and Controls, FTSE 100



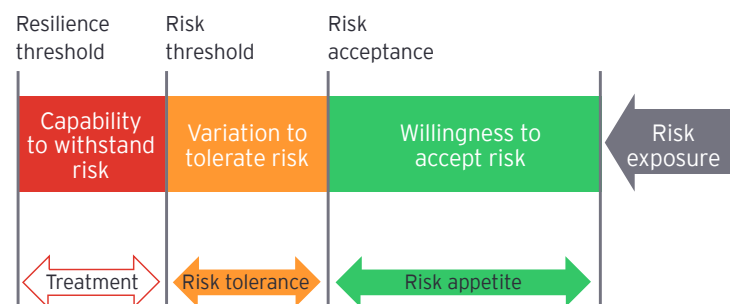


4.2. Agree confidence levels

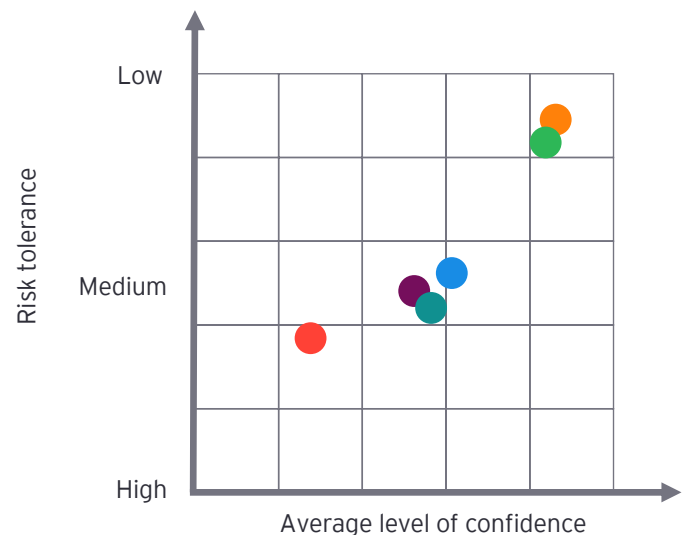
There will be multiple factors that influence the level of confidence directors will require to sign off the year-end declaration, including:

- The category of material control
- How robust the underlying bottom-up transaction level controls are, and what related second-line monitoring activities are in place
- Internal audit priorities and capacity
- The level of tolerance for operating outside of risk appetite

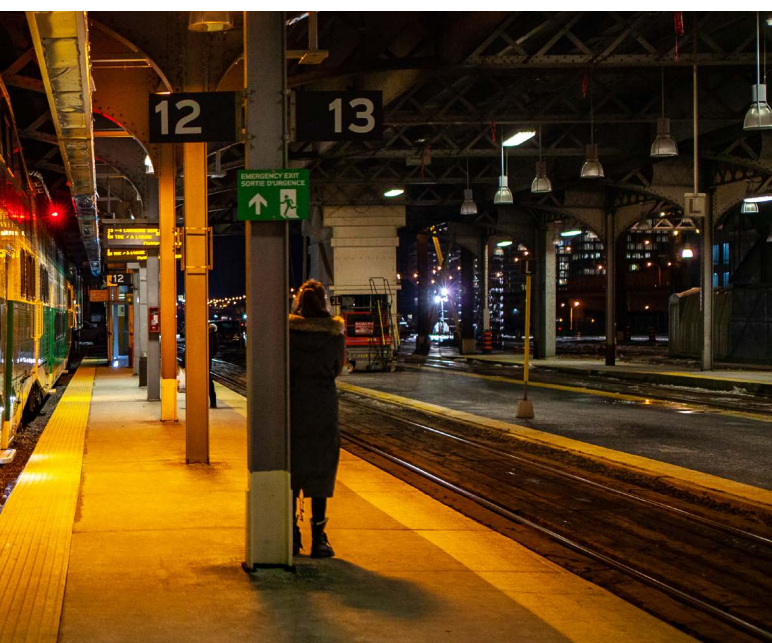
In this context, risk tolerance is the acceptable deviation from the risk appetite for particular risks, expressed in a manner that allows management action to be triggered when it is breached.



Some companies began to map confidence levels or assurance sources against risk tolerance – the lower the tolerance, the higher the level of confidence directors may require:



The initial step in agreeing on what additional activities might be required is often conducting an assurance gap analysis, as referred to in [Ocado's](#) plans for FY25. Our conversations suggest that this is often not a straightforward exercise, as businesses struggle to succinctly articulate the layering of various activities that are already performed in a manner that aligns with material controls.



4.3. Agree sources of evidence

Management needs to agree with directors on what sources of evidence they expect to receive to discharge their monitoring and review duties. There will be a variety of activities undertaken across the organisation contributing to the overall confidence levels. However, directors do not need to be appraised of all of them.

4.3.1. Material control assertions and attestations

In some cases, the board may be satisfied with an effectiveness assertion provided to it by the executive risk owner. The assertion should be supported by concise documentation that focuses on outcomes rather than technical details.

The benefit of this approach is that the executive risk owner is well-positioned to bring together various pieces of source evidence, such as results of control self-assessments and second-line monitoring, that the directors may not be best equipped to interpret for themselves in the context of material control effectiveness. The shortcoming is that the risk owner may be biased towards downplaying any gaps or areas requiring improvement, as this may reflect poorly on them.

Getting the ownership of this conversation about material controls in the executive's own words – including whether they would be comfortable asserting their effectiveness to the Board – is **much** more valuable than subjecting them to a testing regime by a second-line team, and likely to be much more sustainable over time. Judging 'effectiveness' may be highly nuanced for executive leaders, but this thought process is really important for the Board to understand.

Head of Risk and Assurance, FTSE100

A complex challenge that companies have is determining how best to evidence the effectiveness of those material controls that span multiple principal risks. Whilst it makes sense for risk-specific material controls to be reported to directors by the risk rather than the control owner, this is unlikely to work in practice for enterprise-wide controls that address multiple principal risks. A more structured approach, bringing together the control owner, functional leads and entity-level governance bodies, may be necessary to support a view on effectiveness.

Clarifying accountability for cross-cutting, enterprise-level material controls that control against multiple principal risks is one of the more nuanced aspects of Provision 29. Whilst principal risk owners may attest to discrete controls, overarching frameworks often require input from functional leaders or control owners to form a credible group-level view. Aligning industry thinking on how effectiveness is assessed – and evidenced – for such controls would support greater consistency and confidence in board declarations.

Head of Enterprise Risk Management, FTSE100



4.3.2. Effectiveness of entity level controls

As noted in [2.4.3.1](#), it is common for entities to designate existing entity-level controls as material controls. However, being able to assess them for effectiveness may require preparation. Companies are improving the documentation to create better alignment with the principal risks that an entity-level control helps manage. Work is also being undertaken to demonstrate that the controls are truly embedded across the organisation.

Focus on entity-level controls (ELCs)

When designating an entity-level control as a material control, consideration needs to be given to how its operational effectiveness will be assessed and confidence provided to the board. Taking the code of conduct as an example, internal audit can be engaged to perform:

- **Bottom-up testing:** When performing a review at a particular location or division, internal audit will assess operational aspects, such as verifying that employees have access to the current version of the code and examining the record of training completion.
- **Top-down testing:** This requires a dedicated, comprehensive assignment that starts with analysing the extent to which the code continues to be aligned with organisational objectives and continues all the way through to how code violations are dealt with.

The bottom-up approach is certainly more common, but whilst valuable, it may not be sufficient in itself to evidence the effectiveness of the entity-level control across the organisation. The board is likely to require a combination of top-down testing conducted at least every couple of years, supplemented with bottom-up testing in the intervening periods.

Given the nature of the code of conduct-related entity-level controls, the natural choice will be for assessments to be conducted by the third line. Companies that do not have an internal audit function may find it challenging to give directors the confidence they need to declare the material control effective.

David Khalil

EY UK Director, Risk Consulting
dkhalil@uk.ey.com

4.3.3. Controls testing

Companies are referring to enhancing the testing of internal controls, as mentioned by [Phoenix](#) and [Rotork](#). In some cases, this controls testing was limited to financial reporting controls only. Our conversations indicate that more emphasis is being placed on second-line testing activities than on expanding internal audit plans.

There are also multiple references in ARAs to establishing annual testing programmes for material controls. For example, [Grafton](#) states that it will establish an annual programme of testing of all material controls, including key anti-fraud controls, and [Endeavour Mining \(Figure 1\)](#) notes that its material controls will be tested in 2025.

It is, however, not clear from the narrative what that testing will involve, especially in the context of material control categories other than elevated key controls, which might not lend themselves to a traditional testing regime. Some of our conversations indicate that the approach for cluster and framework controls will emulate the approach to checking the effectiveness of entity-level controls.

Assessing the effectiveness of the framework does not hinge on the effectiveness of individual controls within it but on the effectiveness of its broader elements and the outcomes it delivers.

To agree on how a 'framework material control' is going to be assessed for effectiveness, it can be helpful to work backwards by agreeing on what outcomes would lead to a conclusion that the framework was, in fact, ineffective and, from there, determining what could cause such an outcome.

The board can gain confidence about the effectiveness of the framework through a combination of KPI reporting on the outcomes of the framework, activities or controls that indicate the framework is operating effectively, and reporting relating to the activities of the three lines.

Adopting a framework approach often leads to an increased focus on second-line activities and related escalations, which are presently often rare.

Group Audit Director, FTSE 100

4.4. Determine monitoring and review activities

Where levels of confidence and sources of evidence have been agreed upon with directors, we are seeing the conversation move towards setting out the related cadence of reporting.

We view monitoring as an ongoing, proactive activity aimed at early identification of deviations in the functioning of the risk management and internal control framework, and at ensuring that any corrective actions are taken.

Over the course of the year, monitoring will involve both standing agenda items and reporting based on agreed trigger events and will include, for example:

- Key risk indicator dashboards
- Periodic updates about risks and controls
- Risk function presentations and deep dives
- Control self-assessment dashboards and summaries
- Internal audit reports
- Updates in response to risk events or external trends and factors
- Near-miss reporting



289: Where the internal control system only narrowly achieves the desired outcome, especially on numerous occasions during the reporting period, this should be reported to the board. 'Near misses', although not a clear deficiency, can highlight that the control framework is not working as envisaged, and consideration should be given to improving the system.

In contrast, the review is a reflective evaluation designed to reach a conclusion about effectiveness at a time – at or near the balance sheet date in this case. In the context of Provision 29, the review culminates in a declaration on the effectiveness of material controls.

Monitoring and review are interconnected, with monitoring often serving as a foundational input to the review process. For example, ongoing monitoring of adherence to segregation of duties in financial reporting processes provides evidence for a review to assess the effectiveness of the related material control.

The review will often synthesise monitoring outputs, as illustrated by [Drax \(Figure 9\)](#). Its Audit Committee's review is supported by the quarterly risk and control update provided by management. These updates detail any material changes in the Group's principal risks and the associated controls employed to manage them. It also summarises the outcome of management's process of self-attestations and second-line sample testing of key internal controls, as well as other instances where significant weaknesses in internal control have been identified. Finally, updates are provided on the findings from the Internal Audit plan.

Directors need to agree with management on what, if any, updates they require regarding material controls effectiveness if reporting on a particular area was provided earlier in the year. It may be that in some cases, a representation from the risk or control owner will be sufficient; in others, directors may wish to receive additional evidence, especially if monitoring activities indicated weaknesses in a particular material control's operation.

281: The review should consider issues dealt with in reports reviewed by the board during the year, together with any additional information necessary to ensure that the board has taken account of all significant aspects of risk and internal control framework for the year under review and up to the date of the balance sheet.



4.5. Perform a dry run

Very many of the companies we have spoken to have the intention of 'pressure testing' or piloting their theoretical approach in practice before making the first declaration. Performing such a dry run in 2025 will give directors visibility into its potential outcomes and provide directors with the information necessary to visualise what the material controls declaration might look like.

This sentiment is reflected across numerous annual reports:

- [Drax \(Figure 9\)](#) considers an initial dry run of assurance intended to support the internal control declaration to be a key milestone for 2025.
- [Deliveroo](#) anticipates having completed a dry run for the assessment of material controls in 2025.
- [Derwent's \(Figure 8\)](#) initial proposal on material controls will be further enhanced in preparation for a dry run in H2 2025.
- [Centrica](#) intends to pilot the material controls sign-off process in advance of the actual sign-off date, enabling it to refine and test the controls, identify any gaps and ensure their effectiveness.

A dry run is designed to identify gaps and issues in advance, allowing them to be addressed before the first public declaration. We expect that the dry run will also focus minds on the nuanced debate of what constitutes a material control not operating effectively as at the year-end. Generally, companies we have engaged with are concerned about disclosing material control ineffectiveness if other companies take a more lenient view of what that constitutes.

Presently, conversations are focused on the US SOx context: Is any material weakness disclosed for US SOx purposes equivalent to a material control not operating effectively, or is it only the case if the weakness is identified by the external auditor?

4.6. Artificial intelligence (AI)

References to AI are now widespread in ARAs. It is not uncommon for AI to be noted as an emerging risk or referenced as a factor impacting a number of principal risks. Some companies are working towards integrating AI risk reviews into their risk management and internal control framework or developing specific AI governance frameworks, for example:

- [GSK \(Figure 17\)](#) continued to embed its cross-functional AI Governance Council to oversee AI strategy and to ensure the responsible adoption of AI and machine learning. It also introduced a new responsible AI Standard Operating Procedure, which defines the requirements for all development and procurement of AI systems across GSK, and established a framework for business functions to integrate AI risk review and management within existing risk management compliance boards.
- [Pets at Home \(Figure 18\)](#) notes that as AI is being used increasingly across the business to enhance efficiency, support innovation and improve the consumer experience, it brings complex risks and requires controls and guardrails over development, deployment and performance. Its Audit Committee has overseen the development of the AI governance framework, a material control framework, to ensure the framework is appropriate and that the Acceptable Use Policy has been appropriately rolled out across the Group.

Agentic AI

Interview with

Jason Walters

Director, Technology Risk

jwalters@uk.ey.com

What is agentic AI?

Agentic AI refers to AI systems that act autonomously. These systems utilise large language models and machine learning, but go further than generative AI (GenAI) as they make decisions and take actions on their own.

Unlike robotic process automation (RPA), which requires blueprinting of process steps, agentic AI reasons and searches for the best route forward, learning from its context and experience.

It's also different from GenAI, which requires you to initiate a task or submit a prompt. If the result is not fit for purpose, you need to refine your instructions – this takes time and human effort.

For example, whilst RPA can process invoices and GenAI can provide you with a summary of spend with recommendations for cost efficiency, an agent could overhaul the process entirely. An agent – or a group of agents – deployed in purchasing could monitor inventory levels and demand, raise a purchase requisition, evaluate vendors and issue a purchase order.

Why is there so much focus on agentic AI now?

The power of agentic AI to reimagine how processes operate has brought it into focus. The promises of efficiency and productivity gains with GenAI were limited by the need for a human to initiate the inputs and evaluate outputs closely. Agents change the game.

And companies are looking to realise those benefits. Of the UK respondents to the EY Responsible AI CxO Pulse survey, a third (32%) reported already using agentic AI, and 44% planned to deploy agents in the next year.

However, it's not all opportunity. The use of agents requires a fresh look at risk responses and controls.

How does agentic AI change risk?

Many companies have or are looking at risks regarding AI generally, and these considerations continue to be relevant, but they are evolving with agents.

Risks around data governance and privacy are even more important as the reliance on that data increases through the use of agents. Regulation in this area continues to develop at a different pace and with different areas of focus around the globe, adding to the complexity of data and AI compliance.

The democratisation of tools to build agents with low code or no code increases the risk that agents are deployed without the company even knowing, let alone controlling that deployment – often referred to as 'shadow AI'.

Performance risks also increase. Agents require design, deployment and monitoring. Design and deployment are familiar areas of risk for other technology projects; however, with agents and their ability to evolve and respond to their experience, monitoring becomes more complex as companies need to consider whether that algorithm changes over time.

In the example of the purchasing agent ecosystem, the agent responsible for selecting vendors may learn from its historical practice of selecting vendor X and develop its own bias towards that vendor in the future – even if that vendor's products deteriorate in quality. Without robust monitoring, this problem could go unnoticed until it has a significant financial or reputational impact.

How are controls evolving in respect of agentic AI?

Like risks, the control considerations are familiar but augmented. Access management and segregation of duties are key, but they operate differently from before. The roles need to balance the specific agent, other agents in the ecosystem and the human developers of those agents.

Additionally, change management principles can be applied to agentic systems, but they need to be adapted to reflect agentic-specific challenges – for example, explainability (i.e. do I understand why the agent takes the actions it does?) and accountability (i.e. unambiguous ownership of AI systems and their impacts).

The same Responsible AI CxO Pulse survey showed that about half of the CxO respondents in the UK saw their current approach to technology-related risks as insufficient to address new challenges associated with the next wave of AI.

As companies reevaluate their control frameworks in preparation for compliance with Provision 29, we recommend that the evaluation considers how agents will impact IT general controls and financial reporting controls to mitigate the need for rework. This evaluation should also consider what specific steps should be taken to establish robust control over this rapidly evolving area.

Many companies are already appointing chief AI officers (CAIOs) or setting up AI oversight committees. These roles and committees serve to centralise AI. Boards should expect management to have such roles in place or to leverage existing risk officers to specifically cover agentic AI.

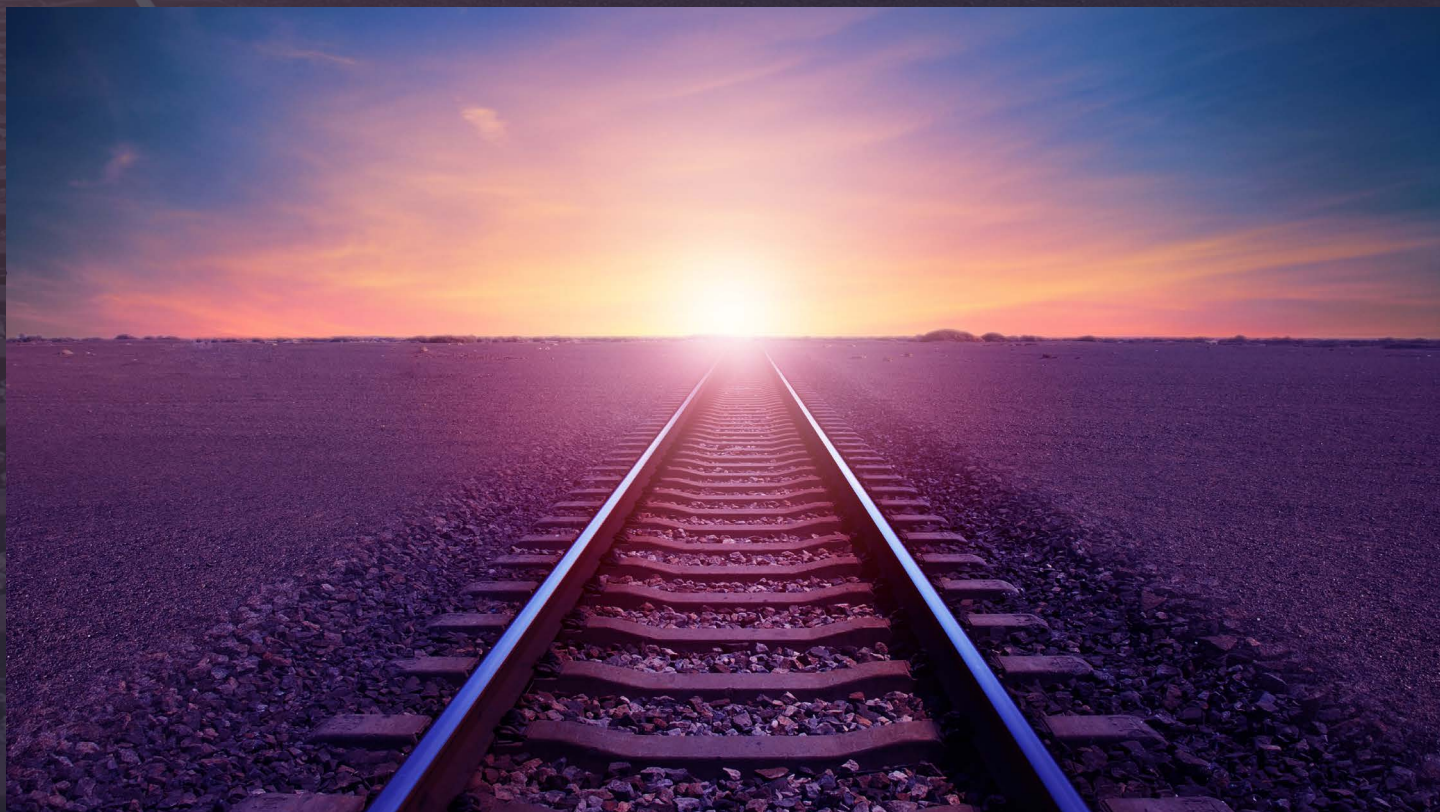
Do you expect companies to have a material control over agentic AI?

Companies need to evaluate the pervasiveness of agentic AI to determine how to respond in terms of material control identification, keeping in mind that a dynamic approach is key.

In the case of the procurement agent ecosystem, many risks and controls are part of the overall purchase-to-pay business process and, therefore, form part of the financial reporting controls. In isolation, it may not be necessary or appropriate to identify a specific material control related to agentic AI.

However, as the use of AI and agents increases in significance to the company, it may become necessary to identify one or more material controls over AI and agents. This is similar to the evolution of cybersecurity controls. The increase in the prevalence of cybersecurity as a principal risk has driven more companies to identify cyber-related material controls.

That said, it may be worth assessing whether to establish a 'material control in waiting' now to enable the company to respond to the rapid changes in this space.



5. Reporting recommendations

5.1. Introduction

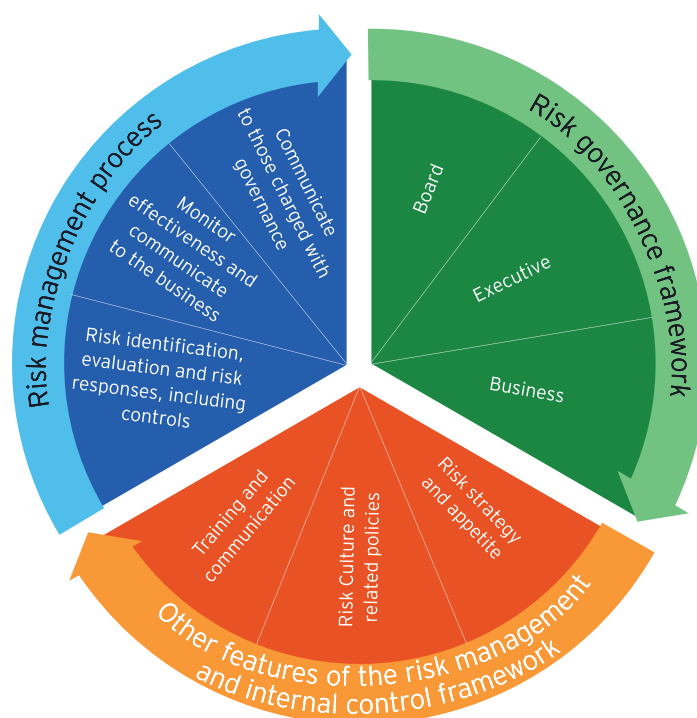
New disclosures in the annual report will be required to comply with the revised Provision 29, and the FRC's Guidance to the Code recommends further narrative to make this reporting meaningful.

293: The board should describe the main features of the 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.

Adding content, especially in the context of an already lengthening risk management section, seems contrary to the multiple initiatives and calls to reduce the length of the ARA and overall reporting burden.

Our analysis of ARAs confirms that the majority of companies already include information about their risk management and internal controls framework. However, the level of detail varies and there is also significant inconsistency in the way terminology is used. We propose a reporting model that distinguishes between the following three elements of the overall framework:



As we had done in our publication in [August 2024](#), we continue to advocate for a logical flow that creates a cohesive narrative. Whilst some new content will undoubtedly be needed, there is scope to remove repetition between the risk reporting in the strategic report and the risk management content in the rest of the governance report and the audit committee's report. If approached well, complying with Provision 29 should not result in substantial additional content.

The recommendations in this chapter should allow companies to tell a compelling story that gives readers confidence in how they manage enterprise and disclosure risk.



Core component	Should include	Specific considerations and top tips
Strategic report		
Overview of the main features of the risk management and internal control framework	Governance structures in place (see 5.2)	<ul style="list-style-type: none"> Directors – requires clarity on allocation of remit related to risks and to controls Management – focus on information flows rather than reporting lines
	Other features of the framework (see 5.3)	<ul style="list-style-type: none"> Provide a high-level overview of risk culture, related policies, training and communication Discuss the board's role in setting risk appetite.
Description of the risk management process	Steps in the risk management process (see 5.4.1)	<ul style="list-style-type: none"> Disclose reporting to those charged with governance as a distinct activity
	Roles within the risk management process (see 5.4.2)	<ul style="list-style-type: none"> Set out who performs and who monitors the operation of internal controls
Activities undertaken by various levels within the organisation, as part of: <ul style="list-style-type: none"> The risk management process disclosure (theory) Principal risk reporting (application in the year) 	Risk identification and evaluation (see 5.5)	Set out: <ul style="list-style-type: none"> Risk taxonomy or categorisation How emerging risk identification differs from that of principal risks Year-on-year changes to principal risks
	Risk responses and how their effectiveness is monitored (see 5.6)	<ul style="list-style-type: none"> Provide an overview of the internal control framework in addition to responses for each principal risk Disclosure Guidance and Transparency Rule (DTR) 7.2.5 Set out sources of confidence over the effectiveness of material internal controls.
Governance report		
Outcomes-based governance reporting	How the board conducted monitoring activities (see 5.7)	Explain what monitoring activities entailed, i.e. the basis (e.g. key risk indicators, dashboards, deep dives, reporting from risk owners), their scope and their outcome.
	How the board conducted review activities (see 5.8)	Explain as at year end: <ul style="list-style-type: none"> How actions arising from prior-period and in-year findings were closed out Whether any final updates or representations were obtained
Culminate in the declaration of material controls effectiveness	(see 5.9)	<ul style="list-style-type: none"> Combine with the confirmation on conducting a robust assessment of emerging and principal risks. Cross-reference to reports from relevant board committee that undertook aspects of the monitoring and review of the framework.

5.2. Risk governance framework

The risk governance framework disclosure should explain the roles and interaction between those charged with governance, executive management and the business and not repeat information included in the overarching governance framework that most reporters include at the beginning of their governance section in the ARA.

Rather, it should clarify the information and reporting flows e.g. from risk owners, the executive committee or other forums such as risk committee to the governance bodies to enable the board and its committees to exercise such oversight. These flows are distinct from reporting and hierarchical accountability lines and therefore may not lend themselves to presentation as an organisation structure. A good example of such a depiction is [Tesco \(Figure 19\)](#).

Some companies effectively demonstrated information flows to governance bodies from the risk and control functions further down in the organisation to allow effective oversight. For example:

[Persimmon](#) enhanced reporting in 2024 to its Audit & Risk Committee regarding the Group's risk management framework, with an update from the Group Internal Control Manager provided regularly to the Audit & Risk Committee.

- What the Board could do better: Instructions and procedures for monitoring business risks and internal financial controls.
- Action: Deliver an initial phase of control enhancements in preparation for Governance Code changes. Routine reporting has been improved, with an update from the Group Internal Control Manager provided regularly to the Audit & Risk Committee. This will continue to be an area of regular engagement for the Committee into 2024.
- Progress made during the year (2024): Enhanced reporting to the Audit & Risk Committee regarding the Group's risk management framework, including principal risk evolutions and control effectiveness, occurred during the year. Regular updates were also provided regarding the Group's programme of work to strengthen the risk management framework and the overall control environment. The delivery of improvements to the Group's risk management framework has been underpinned by the establishment during the year of the Group's Management Risk Committee.

[Persimmon 2024 Annual Report](#), page 98



[GSK](#) clarified that as well as the audit and assurance function, its Audit Committee received regular reporting from principal risk owners and the compliance function on areas of significant risk to the Group and on related internal controls. These reports assess the internal control environment within each principal risk area, including enhancements to strengthen controls.



It is most common to set out the roles within the business by reference to the Three Lines Model:

	First line	Second line	Third line
Responsibility	Day-to-day risk management	Coordinating risk management activities and overseeing the first line to ensure it is effectively designed, embedded and operating as intended.	Provision of independent assurance
Accountability	Senior management	Senior management but often reporting or providing information to those charged with governance	Those charged with governance – typically the audit and risk committee.
Typical functions or roles	Operational management within business units or functions	<ul style="list-style-type: none"> ▪ Risk/ERM function – head of risk, chief risk officer ▪ Compliance functions – head of compliance, head of control, head of governance, risk, and compliance ▪ Legal function – general counsel, chief legal officer ▪ Risk forums, executive risk committees, etc. 	<ul style="list-style-type: none"> ▪ Internal audit – head of internal audit, chief audit officer ▪ Audit and assurance – head of assurance



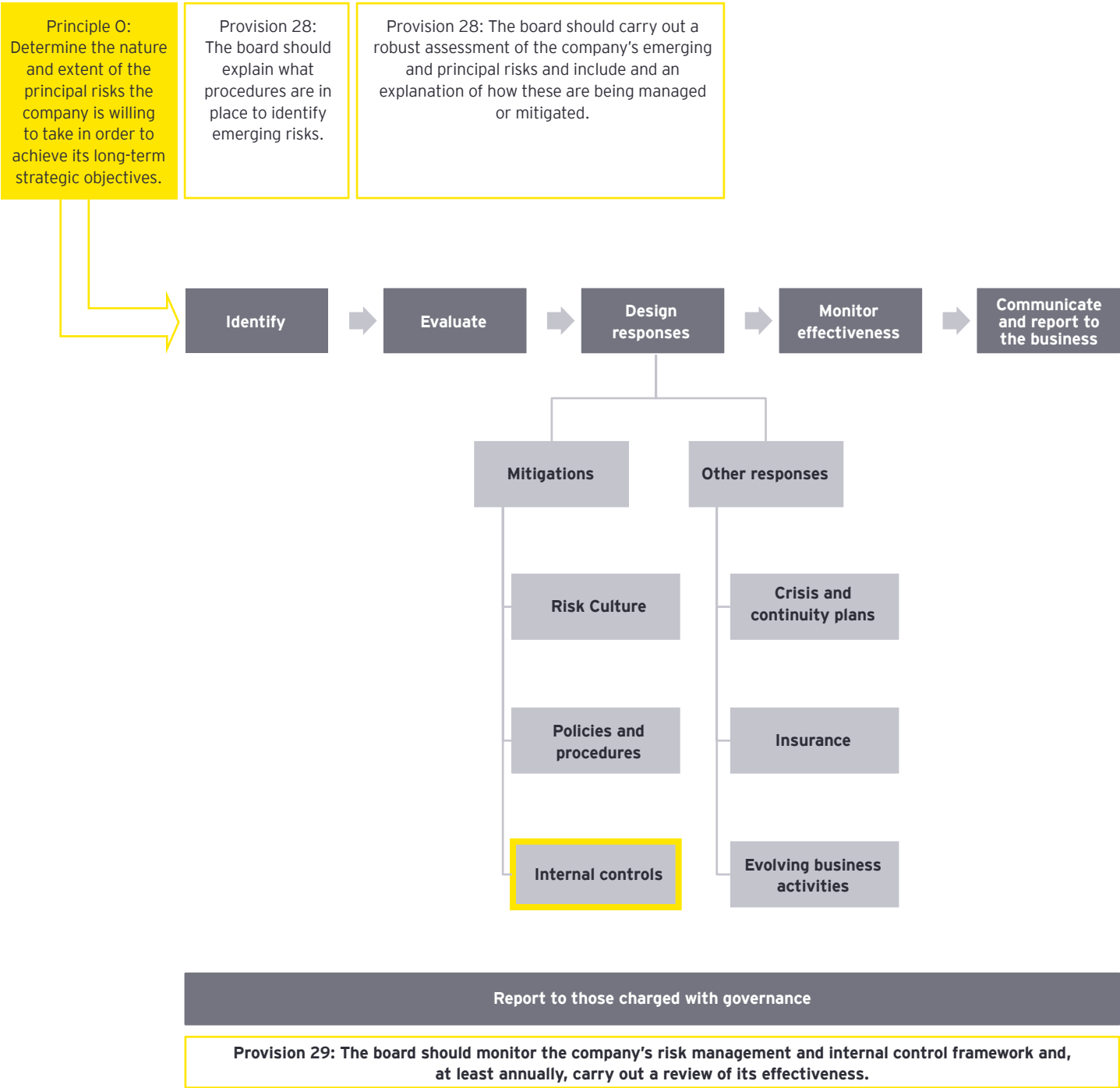
5.3. Other features of the risk management and internal control framework

Other features include risk appetite, risk culture, related policies, authorities, training and communication. Generally, very few companies discuss these features beyond referencing them as part of the role of the board in setting the tone at the

top and determining risk appetite. [Legal & General \(Figure 20\)](#) provides a concise overview.

As noted in [2.3.1](#), only a third of companies disclose risk appetite. Whilst disclosing risk appetite for each principal risk might be considered by some as divulging a company’s competitive advantage, this should not preclude providing a high-level overview of the board’s approach to risk appetite, as done by [PPHE \(Figure 21\)](#).

5.4. Risk management process





5.4.1. Steps in the risk management process

Whilst there isn't a hard and fast rule, at a high level, we expect disclosure of risk management processes to cover the following core steps:

- **Risk identification:** initial identification or at least categorisation of key risk areas. Risk identification and setting risk appetite are iterative. One can shape the other over time.
- **Risk evaluation:** Next, the severity of risks is evaluated, often by reference to the impact and likelihood of the risk manifesting and the risks are prioritised.
- **Developing and designing risk responses:** These can involve mitigating, avoiding, transferring or accepting the risks.
- **Monitoring:** Once response plans are put in place, these plans need to be monitored to ensure that they are working as intended. To increase confidence in the process, additional activities including assurance can be conducted to confirm the effectiveness of responses.

- **Outcomes of monitoring and assurance need to be communicated and reported to those:**

- In the business managing the risks (i.e. the first line) with clarity on any improvements that may be needed
- Charged with governance to allow them to monitor and review the effectiveness of the risk management and internal control framework



Whilst in varying degrees of detail, over 80% of the ARAs we reviewed had disclosure of this nature. From our review, the narrative on risk identification and evaluation is well covered. We recommend that companies review and enhance their disclosures on risk responses and outcomes from monitoring.

5.4.2. Roles in the risk management process

Some companies, including [M&S \(Figure 22\)](#) and [Fresnillo \(Figure 23\)](#), combined the disclosure of the risk management process with a description of who within the business undertook the steps. This approach helps to reduce unnecessary duplication and also provides more clarity into the responsibilities. In this context, it is important to remember that, whilst playing an important oversight role, governance bodies such as boards and audit committees are not a line of defence.

Steps in the risk management process	First line	Second line	Internal audit
Identify and evaluate risks	<ul style="list-style-type: none"> Identifying risks Evaluating risks Monitoring and reporting on their risk profile, e.g. new operational risks or control gaps Reporting on KRIs 	<ul style="list-style-type: none"> Creating and maintaining risk and control standards and policies Assessing and challenging reported risks Identifying and monitoring emerging risks, e.g. via horizon scanning 	
Design risk responses	<ul style="list-style-type: none"> Developing and implementing strategies and 'responses' to manage risk (controls and other mitigating actions) 	<ul style="list-style-type: none"> Assessing and challenging adequacy of first-line responses to ensure risks are being managed within risk appetite, e.g. via a review of KRIs Monitoring the controls implemented and operated by the first line Analysing and reporting on the adequacy and effectiveness of risk management (including controls) and escalating as appropriate – thus providing a degree of management (not independent) assurance 	<ul style="list-style-type: none"> Providing assurance for risk responses (mitigation, controls, etc.) by testing controls, for example
Monitor and communicate	<ul style="list-style-type: none"> Control self-assessments or certifications 	<ul style="list-style-type: none"> Developing and implementing improvement plans in relation to RM and IC Stress and scenario testing in order to assess resilience and test contingency plans Reporting of exceptions and breaches, e.g. against risk appetite, and action tracking Providing support, constructive challenge, guidance and training for the first line, including to embed the right risk culture 	<ul style="list-style-type: none"> Delivering internal audit plan as agreed by governing body Providing independent assurance on the effectiveness of the first and second lines Overall evaluation of internal control environment

5.5. Risk identification and evaluation

5.5.1. Risk taxonomy and classifications

As noted in [2.3.2.2](#), a number of annual reports started to reference the term 'material risks' without providing a definition. If non-standard terms are used, i.e. other than principal risks, the disclosures should clarify definitions and categorisation within the risk hierarchy or taxonomy:

- [3i Infrastructure \(Figure 24\)](#) explains its definition of the term 'key risks'.
- [BT \(Figure 12\)](#) sets out its concept of 'point risks'.
- [Aviva](#) describes Level 1, Level 2 and Level 3 risks and notes this taxonomy provides a consistent basis for assessing, summarising, aggregating and reporting risk, capital and control information.
- [Pearson](#) defines three categories:
 - Principal risks – those that could have a significant and ongoing effect on the Group's valuation by reducing the demand for, or profitability of, its products and services.
 - Significant near-term risks – risks that could have a significant near-term cash impact or affect short-term results but would not be expected to have a significant ongoing effect on the Group's valuation.
 - Emerging risks – risks which are well mitigated in the short term but may represent a significant future opportunity or threat. These include company-specific risks and risks affecting the macro economy.

5.5.2. Risk identification

Provision 28 requires boards to 'explain what procedures are in place to identify (...) emerging risks' without requiring the same for principal risks. Regardless, most companies set out how principal risks are identified, often referencing both a bottom-up risk identification process conducted by the business, and an overlay from a top-down one, typically performed by those charged with governance or by the executive. [discoverIE \(Figure 25\)](#) explains how the two processes are conducted in parallel twice a year.

However, only a few companies explain how, or if, emerging risk identification differs from that of principal risks. Horizon scanning and insights from external publications are commonly noted in such disclosures.

- [Severn Trent \(Figure 26\)](#) references cross-functional workshops, PESTLE analysis⁶ and horizon scanning, which utilises internal insights and external publications, including the National Risk Register and the World Economic Forum's Global Risk Report.
- [Lancashire \(Figure 27\)](#) identifies emerging risk by utilising horizon scans and regulatory-driven enquiries. Its disclosures set out how its emerging risk radar is subject to an iterative process of review and oversight.
- [Fresnillo](#) references the involvement of external parties, including suppliers, contractors and customers, in workshops, surveys and meetings; the use of academic publications; risk consulting experts and industry benchmarks.

5.5.3. Robust assessment of emerging and principal risks – Provision 28

Provision 28 requires the board to carry out a robust assessment of the company's emerging and principal risks and confirm in the annual report that it has completed this assessment. Rather than simply including a confirmatory statement, we recommend companies include brief commentary on:

- The factors considered as part of the assessment – this often included both external and internal factors such as elections; persistent geopolitical volatility; evolution or convergence of emerging risk themes into a principal risk; strategy refreshes etc.
- What the process entailed.
- Its outcomes – providing status updates or disclosing year-on-year changes are ways to demonstrate outcomes and also implicitly evidence the robustness of the process. This is also in line with Principle C, which requires governance reporting to focus on board decisions and their outcomes in the context of the company's strategy and objectives.

Of the reporters that provided such commentary:

- [SSE](#) explained that although its principal risks themselves have not changed, a change in how they were assessed (through dedicated risk workshops and one-to-one stakeholder interviews) enabled more risk-based discussions across oversight committees and Senior Management leading to improved holistic output. It also notes that four risks have increased in materiality.

6. A PESTLE analysis is a diagnostic tool to assess the impacts of macro-environmental factors on an organisation. PESTLE is an acronym for: Political; Economic, Social, Technology, Legal, Environmental.

- [Lancashire \(Figure 27\)](#) clarified that the oversight of certain emerging risks (e.g. climate change, operational strain, geopolitical risk, inflation, tax and regulatory change), moved to its business-as-usual risk management processes. As a result, emerging risk discussions predominantly focused on the many different components of AI and its risk appetite for utilising them.
- [Harworth](#) noted that its Board had continued to assess principal risks closely, particularly in light of its strategic 'pivot' towards Industrial & Logistics development and investment announced during the year; and external factors such as the election of, and rollout of policies by, the new UK government. It commits to undertaking a comprehensive review of principal risks during 2025, informed by the strategic pivot. It also details the changes to its principal risks since its 2023 ARA.
- [Morgan Sindall \(Figure 28\)](#) provided a status update for each of its principal and emerging risks, and with respect to the latter, included commentary on outlook.
- Similar to [Premier Foods \(Figure 5\)](#), [IWG](#) also took the opportunity to streamline its principal risks reducing the number from 19 in 2023 to 12 in 2024 by removing some and merging others. On average, companies disclose between nine and 12 principal risks.



5.6. Risk responses

Provision 28 requires a description of a company's principal risks, and an explanation of how these are being managed or mitigated. It also requires an explanation of what procedures are in place to manage emerging risks.

As noted in [2.1](#), some principal risks are outside of a company's control. It might therefore be helpful, as done by [British Land \(Figure 29\)](#), to distinguish between external, non-controllable versus internal principal risks. Similarly, not all mitigating responses qualify as controls. Helpfully, for each of its principal risks, [Glencore \(Figure 30\)](#) describes the mitigations that are inherent within its business model and those that are implemented as controls. [IHG \(Figure 31\)](#) provides illustrative examples of key controls categorised between culture and leadership, processes and controls, and monitoring and reporting.

From our analysis this year, we note that rather than just referring to broad mitigating actions or activities, 13% of principal risks disclosures referred specifically to controls, for example:

- Control environment – [Rathbones](#)
- Key elements of internal controls – [Rightmove](#)
- Key controls [Morgan Sindall](#) and [JTC](#)
- Example mitigations and material – [St. James' Place](#)

Whilst there is no requirement to make such disclosures (or indeed to disclose material controls), we recommend that companies review the extant wording of their mitigating activities as readers may interpret or infer controls disclosed therein to be material controls. To avoid this, in its disclosure, [United Utilities \(Figure 32\)](#) clarifies that only those principal risks classified as material impact risks will have associated material controls and clearly differentiates between material controls, other controls and other mitigations in its principal risk disclosure.

Despite the requirement, disclosures on how emerging risks are managed were sometimes omitted. Where provided, these ranged from:

- An overall description as provided by [Fresnillo](#). This noted the need to be dynamic, reflecting the findings from its monitoring and scenario analysis; keeping abreast of technological advances in the mining industry and beyond; drawing on new sources of information and working closely with universities specialising in mining and geology.
- Commentary against each emerging risk when these are voluntarily disclosed – as provided by [Severn Trent \(Figure 26\)](#) and [Morgan Sindall \(Figure 28\)](#).

5.6.1. Overview of the internal control framework

Whilst most companies disclose the steps in the risk management process (albeit to varying degrees of detail), less than a third (30%) meaningfully describe the principal features or elements of their internal control framework. Some companies that do include [Bunzl \(Figure 33\)](#), [IWG \(Figure 34\)](#) and [Spire Healthcare \(Figure 35\)](#).

Commonly described in these disclosures were:

- Delegations of authority
- Budgeting and forecasting disciplines
- Defined approval authorities, e.g. for major capex and acquisitions
- Group-wide policies, such as codes of conduct, whistleblowing, anti-bribery, etc.
- Activities by the second- and third-line functions as noted in [5.4.2](#).

Given the requirement in Provision 29 for the board to monitor and review the effectiveness of the risk management and internal control framework, we recommend clear disclosure in the strategic report on the constituents of the internal control framework. Commentary in the governance section (e.g. audit committee's report) should then focus on the oversight exercised.

5.6.2. Main features of the internal control and risk management systems in relation to financial reporting process – DTR 7.2.5

Unlike [Spire Healthcare \(Figure 35\)](#), many companies seem to have lost or dropped this disclosure somewhere along the way. It remains a requirement in the DTR 7.2.5 even after the UK Listing Rules reform. Unless financial reporting-related risks are specifically designated as a principal risk, it would not be covered by any other disclosures. There is also a good opportunity to tie together this disclosure requirement with the work on reporting-related material controls given the 2024 Code's expansion to cover reporting.

We recommend that this disclosure complements the overall internal control framework disclosure discussed in [5.6.1](#) by adding specific detail on financial reporting controls, for example:

- Experts that monitor new accounting standard pronouncements, assess their impact on the company's financial reporting and reflect them in the group accounting manual

- A maintained and promulgated group accounting manual
- Training for finance teams
- A range of prevent and detect controls, including segregation of duties, reconciliations, approvals, management reviews and exception reporting to ensure complete, timely and accurate recording of transactions and safeguarding of assets
- An annual budgeting exercise coupled with longer term rolling forecasts which include breakeven and sensitivity analyses
- Specific internal audits, for example to review the integrity of divisional or BU management accounts



5.6.3. Sources of confidence over the effectiveness of internal controls

As noted in 4.2, directors will require a level of confidence in the effectiveness of material controls to sign off the year-end declaration. This will be influenced by the various monitoring, testing and other activities conducted over the operation of internal controls more broadly. An increasing number of companies are now including this information and common sources referenced included:

- Control self-assessments and attestations from within the business or first line:
 - [SSE](#)'s Audit Committee considered the letter of assurance evaluations completed by the managing directors of each of its business units and the directors of corporate functions.
 - [Intertek \(Figure 36\)](#) sets out its approach to self-assessments, including consolidation at divisional, regional and functional levels for further review and sign-off.
- Second-line testing:
 - [Serco](#) described that there is an annual programme of work focusing on the validation and testing of key controls to supplement annual control self-assessments and biannual compliance assurance attestation statements.
 - [Fresnillo \(Figure 23\)](#) notes that the risk team annually reviews key controls for principal risks
- Third-line assurance:
 - [IHG \(Figure 31\)](#) denoted, for each principal risk, what independent assurance was derived from Internal Audit.
 - [Mears \(Figure 38\)](#) described when each of its principal risks were addressed in the Internal Audit plan.
- External assurance to supplement third line activity:
 - [Serco](#) noted assurance activities and audits delivered through external third parties to support certification standards (e.g. ISO).
 - [Fresnillo \(Figure 37\)](#) described external sources of confidence in respect of two of its 15 principal risks – tailings dams and environmental incidents. These sources include ISO certifications; compliance with an internationally issued code with associated certification; and compliance with an annual review programme issued by an independent expert panel which also inspects its compliance and issues corrective and preventive recommendations.

The management of our key controls forms a critical part of our ERM framework. Group and Divisional Compliance Assurance teams operate as a second line function to ensure appropriate focus on the articulation, monitoring and testing of key controls, supported by documented policies and procedures held within our Serco Management System (SMS). An annual program of work focuses on the validation and testing of key controls to supplement annual control self-assessments and biannual compliance assurance attestation statements. Some larger contracts and business units (BU) also have embedded risk and assurance resources to strengthen our first line focus on controls design and operation. This first and second line activity is augmented by our in-house Internal Audit assurance work and additional external partners support in certain specialist areas. Significant third line assurance activities and audits are also delivered through external third parties to support certification standards and customer requirements in our varied service lines and business units. These include those that support ISO certifications we manage as well as independent performance and regulatory reports on Serco operations. Examples of such reviews include Aviation Air Traffic Services, Vessel reviews, Fleet Operating Licence and related inspections. A key element of our control environment in our North America Division is compliance with the Special Security Agreement, we have with the US Government which is managed by dedicated resources and oversight delivered by the Serco Inc. Audit Committee.

[Serco 2024 Annual Report](#), page 62



5.7. Board monitoring activities

Whilst Provision 29 of the 2018 Code required boards to monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness, the disclosure requirement was limited to the board's review and was vaguer, simply referencing the need to 'report on that review in the annual report'.

New in the 2024 Code is a requirement to describe how the board has both monitored and reviewed the effectiveness of the risk management and internal control framework.

From our conversations, this requirement has not received as much attention as the declaration on the effectiveness of material controls which has taken centre stage thus far. It is broader than the declaration and encompasses all elements of the framework described in 5.2 and 5.3 – hence why we recommend clear disclosure of the framework as the foundation to describe how the board monitored and reviewed it.

Good monitoring disclosures should explain not just what information was received by governance bodies (see earlier reference to information flows in 5.2), but also the outcome. Based on our reviews, this is rare to find. We recommend companies clearly describe what action was taken, for example, by an audit committee or requested by it of management following the review of such information.

5.7.1. Key risk indicators

We noted increasing reference to key risk indicators with some companies disclosing these, such as:

- [British Land \(Figure 29\)](#) disclosed clear performance measures to monitor each principal risk.
- [Rathbones](#) noted that risk indicators are developed for each principal risk to provide an early signal of increasing risk exposure. Thresholds dictate an early warning trigger, a breach of risk tolerance through to invocation of the recovery and resolution plan.

However, as described above, disclosure on actions taken by governance bodies following their review of such indicators was rare.

[Derwent](#) stated that the risk indicators (covering 10 risk areas, including cyber security, cost inflation, project status, data protection, and health and safety incidents etc.) are reviewed at each Risk Committee meeting and are compared against the Board's risk appetite statement. Any deviation or significant increase is subject to challenge by the Risk Committee. Specifically in relation to data protection, as part of its key risk indicator schedule, the Audit Committee monitors the number of 'near miss' data breaches and how these have been addressed.

5.7.2. Other monitoring activities

Audit committee reports often referred to the following through the course of the reporting cycle:

- Internal audit reports for the period, as well as progress of actions against prior-year observations.
- Quarterly updates from the third line summarising the results of self-attestations, e.g. [Drax \(Figure 9\)](#).
- Reviews of any major findings into control weaknesses and management's response in reports tabled by heads of Internal Audit.
- Follow-up with management on the rectification of identified control weaknesses.
- Risk deep-dive reviews – [Morgan Sindall \(Figure 28\)](#) provided detail of the deep dives conducted, linking these to relevant principal risks.
- [Helios \(Figure 39\)](#) presents an example controls dashboard and notes that its Audit Committee has a standing agenda item to review internal controls including such a dashboard.

Given the requirement for boards to disclose how they monitored the effectiveness of the framework, we emphasise the need for specificity in disclosures to describe both the underpinning or rationale for these monitoring activities as well as their outcomes. For example:

- What drove the choice of risk deep dives (specific triggers vs. coverage as part of a rolling cycle) and what did the deep dive entail – a challenge of risk appetite, a review of risk responses or an update of the risk profile?
- What was the outcome of a deep dive, a review of a summary of control self-attestations or a dashboard?

Examples of outcome-focused reporting include:

- [British Land](#)'s Executive Risk Committee conducted a survey to assess the robustness of the company's risk culture. Following the outcome of the survey, action was taken to enhance risk culture across the business involving the Head of Risk and Internal Control presenting to various teams across the business, clarifying the key risk roles in the business, and encouraging escalation of risk issues or exceptions, and discussing key business unit risk.
- [Phoenix](#) commissioned an external review of its risk management framework, recommendations of which were presented to its Audit and Risk Committee. The Committee requested a plan to deliver these recommendations and will monitor against this throughout 2025.
- [Drax \(Figure 9\)](#) noted that the outcomes of the key control self-assessments indicated that incomplete or inaccurate supplier data was in some instances delaying due diligence procedures. The Audit Committee agreed that resources should be dedicated to remediating this control ineffectiveness as a priority.

5.8. Board review activities

281: The review should consider issues dealt with in reports reviewed by the board during the year, together with any additional information necessary to ensure that the board has taken account of all significant aspects of risk and internal control framework for the year under review, and up to the date of the balance sheet.

As noted in [section 4.4](#), monitoring and review are interconnected and, in most cases, reporting does not distinguish between activities undertaken as part of one or the other. Making this distinction is not necessary; however, it is important that disclosures ‘close out’ any actions from monitoring activities that occurred earlier in the year, and from the prior period. This could include, for example, disclosing whether a final update report or representations were obtained, as done by [M&S \(Figure 22\)](#), which discloses direct confirmations to the Audit and Risk Committee on the management of key risks.

In terms of period-end activities, i.e. to review the effectiveness of the framework, committees and boards reference year-end reports on various aspects of the internal control environment of the business from internal audit, the risk and finance function, for example:

- [British Land](#) refers to the Audit Committee receiving an exception report from the bi-annual sample testing performed by the Head of Risk and Internal Control on key operational and financial controls.
- [Admiral \(Figure 40\)](#) revised its approach in relation to its annual assessment of the system of risk management and internal control in preparation for the 2024 Code. As well as placing reliance on the third line, in 2024, the Group Head of Internal Controls and Group Chief Risk Officer presented an annual assessment to the Audit Committee.
- [Trustpilot \(Figure 3\)](#) noted remediation of the findings from its review of ICFR were tested by Internal Audit in Q4 2024 and Q1 2025.

5.9. The directors’ 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 [5.6.3](#), [5.7](#) and [5.8](#)), 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 its monitoring activities during the course of the year had been adequately remediated. These monitoring activities combined with 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.

We recommend that the declaration:

- Is included within the overall governance statement, not within one of the board committee reports.
- Immediately follows the basis, i.e. how the board monitored and reviewed the effectiveness of the framework ([5.7](#) and [5.8](#)) and its sources of confidence in respect of material controls effectiveness ([5.6.3](#)).
- Cross-references reports from relevant board committees that undertook aspects of the monitoring and review of the framework.
- Is combined with the confirmation required in Provision 28 on conducting a robust assessment of emerging and principal risks.

5.9.1. 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 disclosures of 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 judgment, contain confidential information or any other information that could inadvertently affect the company's interests if publicly reported.

If challenges and weaknesses in material controls emerge as a result of testing or from dry runs conducted in 2025, we recommend that these are trailed in 2025-26 ARAs as areas requiring action. This will avoid a cliff-edge or surprise, should they remain ineffective at the time of the first mandatory declaration. [RHI Magnesita](#) provides such disclosure.

The reports by management and Internal Audit, Risk & Compliance also facilitated consideration by the Audit & Compliance Committee of management actions in respect of the following key control framework challenges:

- Improving management and the internal controls of transformational initiatives.
- Effective integration of acquired entities into the Group's culture and internal control framework.
- Benchmarking the internal control performance across the regions.
- Continuing the journey towards global process standardisation.

[RHI Magnesita 2024 Annual Report](#), page 52

5.9.2. Providing explanations

Whilst we would not expect boards to explain against the requirement to disclose how monitoring and review of the framework was performed, in some cases, they may caveat that the declaration does not cover certain material controls or that they could not determine the effectiveness of material controls over certain areas. 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 the health and safety framework (as a single-risk framework material control) may not yet cover the health and safety risks in respect of a newly acquired business.

In such cases, the explanation should follow Principle C of the Code. In addition, the following from the introduction to the Code is helpful: *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.*

Using the example above, a board could explain that a temporary material control(s) has been put in place in respect of safety risks in the newly acquired business to cover the period of post-acquisition integration and that it expects the health and safety framework will cover all parts of the business by the time of the next declaration. For clarity, declaring that a material control had not operated effectively as at the year-end is not 'non-compliance' – this is covered by the separate requirement in Provision 29 as discussed in [5.9.1.](#), i.e. to provide a description of any material controls which 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.



Appendix: Illustrative examples

Figure 1

Endeavour Mining 2024 ARA, p. 122

Audit and Risk Committee report Continued	
Internal Controls project in preparation for the 2024 UK Corporate Governance Code (“2024 Code”)	
<p>Management considered the changes to the risk management and internal control requirements introduced by the 2024 Code, (effective from 1 January 2026), to be an opportunity to refresh and enhance Endeavour’s existing Enterprise-wide Risk management process and controls.</p> <p>With support from an external consultancy firm, we have created a risk and control matrix, which identifies the material financial, operational, reporting, compliance and other risks and controls across all our main business processes. This outcome was achieved by undertaking an extensive series of risk and control workshops, involving a mix of financial, operational, reporting and compliance staff from across the business and from all levels of seniority. We also performed a “deep dive” on the more complex processes, to ensure all risks were fully covered.</p> <p>The material risks identified represent a consensus view, based on input from the relevant staff across the business including all functions and departments of the Company. In order to comply with the 2024 Code, material risks and controls will be tested in 2025. Throughout this process a small number of gaps were also addressed with compensating controls and in each case, remediation tasks were agreed with the relevant control operators and target completion dates set. As at the year-end we had completed design effectiveness testing for all our material controls.</p>	<p>In parallel, we developed a Governance, Risk and Compliance (“GRC”) tool, to automate the entire Enterprise-wide Risk Management process. All material controls have been loaded into the tool, which will be used to retain evidence of the operation of the controls and subsequently record operating effectiveness testing (from early 2025 onwards). The opportunity was also taken to enhance and formally document our Enterprise-Wide Risk Management processes covering: Principal Risk Assessment; Corporate Risk Assessment; Fraud Risk Assessment; and Self-certification. As at the year-end these enhanced processes were being finalised with management and will be rolled out in the first half of 2025. The GRC tool will support the day-to-day operation of these processes. The new oversight and reporting model is set out in the diagram on page 120.</p>

Source: https://edv-14806-s3.s3.eu-west-2.amazonaws.com/files/7617/4124/4823/EDV_AnnualReport2024_Website.pdf

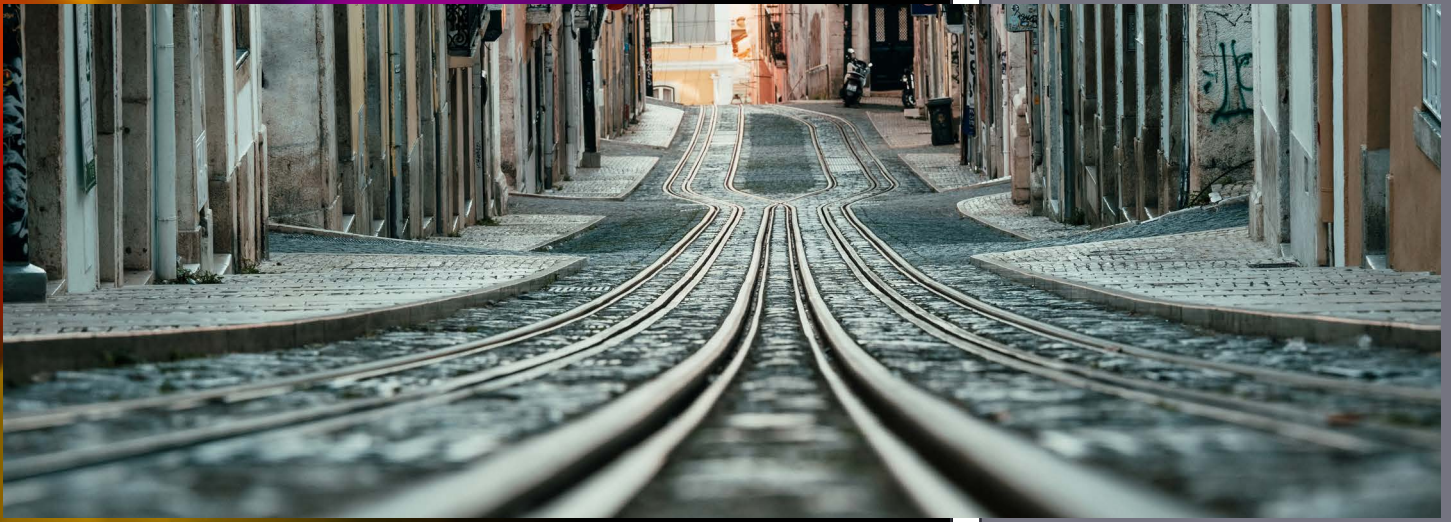


Figure 2

Hunting 2024 ARA, p. 130

Roadmap to compliance with the 2024 UK Corporate Governance Code

The 2024 UK Corporate Governance Code ("2024 Code") was published in January 2024, with the Directors reviewing the key changes to the Provisions and Principles early in the year.

The Directors will be reporting the Company's compliance with the 2024 Code, with the exception of Provision 29, in the 2025 Annual Report and Accounts, to be published in March 2026.

Policies

In 2024, the Group's central compliance function completed a review process of the Group's policies, in line with the requirement of Principle A of the 2024 Code.

The Directors are satisfied that appropriate policies covering all key operational, financial, and compliance matters are in place.

The Group utilises a Group Manual, which contains all of the key accounting policies and procedures, which is also being revised in the year, ahead of 2026, when Provision 29 is to be reported against.

Culture

The Directors approved a framework to monitor and report on culture, in line with Principle C of the 2024 Code. The Board, through the Ethics and Sustainability Committee, has agreed that the metrics noted on page 124 will be adopted for reporting across the year. Further, the Board also agreed that each Director would increase visits to key facilities to ensure the views of employees are directly fed to the Board going forward, in parallel to the use of the Gallup Q12 survey, which is to be repeated in 2025.

Risk management

During the year, the Group's risk management procedures have been enhanced, following the appointment of a Group Risk Manager in 2023.

New risk identification processes were introduced, with the Directors completing a risk workshop to agree the strategic and principal risks facing the Group, as the Hunting 2030 Strategy is being executed.

This has led to a fully integrated risk management framework being implemented across the Group which covers financial, operational, and compliance risks, including climate and environmental risks.

In 2025, further work on the Group's risk universe and culture will be completed.

The Group has also commenced workshops with each of the product groups and operating segments in support of this work.

These workstreams have directly interfaced with the work on internal control noted below.

Internal control

Provision 29 of the 2024 Code requires boards to monitor and review their company's risk management and internal controls. We are aiming to report our compliance with Provision 29 within the 2026 Annual Report and Accounts, to be published in March 2027.

In the year, a process to identify material controls across the Group commenced, including the determination of the internal controls over financial reporting and entity level controls. A review of Group IT controls was also undertaken and an initial determination of non-financial controls, including QAHSE information and compliance procedures was commenced.

A Group Internal Controls Manager was appointed in mid-2024 to assist in the review and documentation of the Group's internal controls, and in January 2025 a new software platform (AuditBoard) was purchased, which will be used by the Group's central finance and internal audit functions to assess compliance and provide internal assurance to the Board about the Group's internal control environment.

As part of the review of the Group's internal control environment as part of the compliance procedures for the 2024 UK Corporate Governance Code, we will also look to address some of the control deficiencies identified in the 2024 year-end audit.

In January 2025, a Group IT Systems Manager was also appointed to commence the standardisation of the D365 ERP system, to enhance consistency of reporting across the Group's business units and to input into the wider financial controls enhancement, which is being undertaken.

In H1 2025, it is anticipated that preliminary testing of assurance procedures against a number of material financial controls will be completed, prior to wider roll out.

Remuneration

In 2024, the Company gained strong shareholder approval for the new Directors' Remuneration Policy ("Policy") and Long Term Incentive Plan.

The new Policy was drafted with the requirements of the 2024 Code in mind and contains malus and clawback provisions (Provision 37).

On behalf of the Board

Stuart M. Brightman
Company Chair
6 March 2025

Figure 3

Trustpilot 2024 ARA, p. 49, 104, 111

Enhancing our management of risk

To improve the customer experience and enhance the integrity of the platform, we've implemented new technologies and processes, including AI solutions. At the same time, we are also evolving our governance and risk framework to ensure appropriate oversight and management of our risks.

In the second half of 2024, we conducted a full review of our functional risk registers, reviewing the alignment between our functional risks, our strategy and our principal risks and uncertainties. We used the opportunity to reaffirm the ownership of risks and controls, ensuring that cross-functional dependencies are mapped and understood.

Additionally, we established closer working relationships between our Trust & Transparency and Technology functions. This included deepening the links at a management level by creating the role of VP Technology with a specific remit for Trust. The role has dedicated ownership and accountability for the technology used to tackle misuse of the platform and works closely with the Trust & Transparency function. Mandatory Data Ethics and AI training was also introduced for all trustees as part of our annual cycle in 2024.

We strengthened our governance, launching our new privacy governance model, establishing a Security, Privacy and Legal Steering Committee and introducing a standardised approval process for the use of machine learning (ML). Additionally, dedicated engineering teams have enhanced our safeguards relating to the use of ML.

Enhancement of our risk function

H1 2024 saw a new Head of Enterprise Risk join the business. Following their appointment, the risk function was refreshed, starting with a robust review of our risk processes, followed by discussions being held with senior leaders to help inform the development of our Enterprise Risk Framework. The structure and hierarchy of functional risk registers was revised to better align with the organisational structure with corresponding revision of the roles and responsibilities of the reporting lines. These changes helped provide greater clarity on the business' principal risks and uncertainties and their potential impact on fulfilment of our strategy. The Committee undertook an in-depth review of the Group's risk plan and work undertaken during the year. Further information on the work of the Risk function during 2024 can be found on pages 48 to 58. The work undertaken on the Enterprise Risk Framework has well-positioned the Company ahead of the UK Corporate Governance Code 2024.

Working closely with the Internal Audit function and external consultants, our Internal Controls over Financing Reporting were reviewed, strengthening the effectiveness of our control environment as we prepare to make the relevant UK Corporate Governance Code 2024 material controls effectiveness declarations from 2026.

The Audit & Risk Committee welcomed reports and presentations at each of its meetings in 2024 from the Risk and Internal Audit function, providing the Committee with the opportunity to get a full understanding of the risk environment of the business and to challenge and support the function.

Systems of risk management and internal control

Risk engagement	Focus and key outcomes
Review of functional risks and controls	<p>The Risk function worked with key stakeholders and Risk Champions across the first line of defence ('1LoD') to review and refresh all functional risk registers. The review included the identification of new and emerging risks and a review of the effectiveness of the control environment.</p> <p>Through this process we have reviewed the alignment of our risks and controls against our strategic priorities and ensured that cross-functional dependencies are mapped. This was designed to support the effective prioritisation of risk mitigation activity whilst also informing the identification of Trustpilot's material controls, in readiness for the changes to the Corporate Governance Code from FY26.</p> <p>The review was also used as an opportunity to reaffirm accountability for management of risk among the 1LoD. The thorough review process has informed our assessment of our principal risks and uncertainties.</p>
Mandatory ethics & compliance training	<p>We expect and encourage Trustees to do the right thing, even when nobody is watching. Our vision to become the universal symbol of trust for consumers and businesses means that our own conduct and reputation must be beyond reproach, and this informs all aspects of our approach to ethics and compliance. We rolled out our expanded mandatory ethics and compliance training to all Trustees, and achieved 100% completion amongst eligible Trustees and contractors in the period. This further matures our risk culture as well as setting the tone around our key policies and expected behaviours. The Risk function ensures that any whistleblowing or reportable incidents are escalated to the Audit & Risk Committee.</p>
Policy management	<p>The Risk function continues to maintain the Group's policy management framework. This includes ownership of the policy library which ensures effective oversight, ownership and regular review of our 'core' policies.</p>
Review of internal controls over financial reporting	<p>We carried out a review of our ICFR framework, which assessed the completeness and effectiveness of our control environment as it relates to each key financial process. This is part of a regular review cycle and we were pleased to note continued improvement.</p> <p>Remediation of the findings noted from this review were tested by Internal Audit in Q4 2024 and Q1 2025.</p>
Fraud risk assessment	<p>We maintain a regular cycle of review over our fraud risks and in Q3 we carried out a full refresh of our fraud risk register and fraud risk framework. The findings will help to ensure we are compliant with the new corporate criminal offence of 'failure to prevent fraud' which was introduced as part of the UK's Economic Crime and Corporate Transparency Act ('ECCT') and will come into force on 1 September 2025.</p>
Risk mapping with our ELT	<p>The Risk function facilitated a workshop for the ELT to prioritise our principal risks and uncertainties, by considering the potential impact and probability of the related events or circumstances, and the timescale over which they may occur.</p>

Figure 4

Howden Joinery 2024 ARA, p. 148

Case study

Preparedness for the UK Corporate Governance Code changes (risk management and internal controls)

The 2024 version of the UK Corporate Governance Code has introduced a new Provision (Provision 29), requiring boards to monitor their company's risk management and internal control framework and, at least annually, to conduct a review of its effectiveness. For financial years beginning on or after 1 January 2026, a description of how the board monitored and reviewed the effectiveness of the framework, a declaration of the effectiveness of material controls, and a description of any material controls that have not operated effectively (including action taken or proposed to improve them) must be reported in the annual report.

In readiness for these changing requirements, Howdens has completed a two-year Company-wide readiness project. Sponsored jointly by the CEO and CFO with the oversight of the Audit Committee, the Key Controls Project was a wide-reaching improvement programme to further improve our governance, controls and evidence. A key objective of the project was to retain Howdens' culture of empowered, entrepreneurial teams operating efficiently while demonstrating effective control and governance.

Our approach mapped our principal risks as well as wider legal, financial, compliance and operational risk areas to a revised governance framework with clear accountability for each Executive Committee member. To do this we have revised our risk appetite matrix and developed a clear link to both operational and financial materiality, ensuring that our governance approach focuses on truly material

controls, while allowing the business to keep track of its wider operational control effectiveness.

For each area, a control framework was developed, focused on providing the Executive member responsible with appropriate information and evidence to ensure it remains effective. Directly aligned with our deeply embedded risk management process, all control owners and reviewers are responsible for understanding individual, evidenced risks in their area and signing off that controls are effective and have fully operated during the period.

Throughout the project we have aimed for a clear and efficient process, covering governance and controls to manage both Economic Crime and Corporate Transparency Act 2023 (ECCTA) and the revised UK Corporate Governance Code in one simple process. We have upgraded our governance, risk and compliance (GRC) tooling, which was already familiar to the business, to provide both management sign-off of control effectiveness and evidence management to support it. Our GRC solution is directly linked with our 3rd line Internal Audit activity, providing a clear link between control sign-off, review and assurance activity for the Executive Committee and Audit Committee.

We are continuing to develop our compliance functions to align against this new model and to ensure that this approach is effective.

Material controls

As previously reported, management continued a Group-wide controls and governance oversight improvement project in 2024. Sponsored by the CEO and CFO, and reporting regularly to the Audit Committee, this work is improving our capability over our operational, compliance, IT and financial controls, which mitigate our key and principal risks and evidence their effective implementation.

Work on tightening and evidencing our IT and financial controls was largely completed in 2023. In 2024, the focus has been on rolling this out to all other areas of operations and governance, with regular updates being provided to the Audit Committee. Work has focused on refining embedded internal control frameworks and reporting, as well as our systems used to improve process efficiency and the use of data analytics.

The Committee remains committed to the activities to further strengthen the control environment across the business, as well as preparing for compliance with Provision 29 requirements of the updated 2024 version of the UK Corporate Governance Code (see case study above).

Internal audit

The Internal Audit team has focuses on the development of our processes and frameworks to align with both new Institute for Internal Audit (IIA) standards and the requirements of the function for the revised Corporate Governance Code. This has included training for the full team and the wider business.

An updated Internal Audit Charter has been approved by the Committee and communicated to management, thereby refreshing understanding of responsibilities for internal controls and their verification, based on the three lines of defence model.

Source: <https://www.howdenjoinerygroupplc.com/docs/librariesprovider25/archives/annual-reports/2024-annual-report.pdf>



Figure 5

Premier Foods FY25 ARA, p. 59-60, 86-87

Effective risk management protects our business and complements our strategic decisions as we strive to grow the business.

Our approach

Our Board owns and oversees our risk management programme. It is responsible for ensuring that our risks are aligned with our goals and strategic objectives. The Audit Committee assists the Board in monitoring the effectiveness of our risk management and internal control policies, procedures, and systems.

We have historically followed an established risk management framework to identify, evaluate, mitigate and monitor the risks we face as a business. Our approach is both top-down and bottom-up to ensure that

we have maximum input from the Board and from operational management. Our objective is not only to identify current and emerging risks that our business faces as we execute our strategy and grow the business, but also to ensure that consideration of risk is embedded in our strategic decision-making.

Operational responsibility for risk management is embedded throughout our organisation and our first line of defence remains our colleagues, who have a responsibility to manage day-to-day risk in their areas guided by Group policies,

procedures, and controls frameworks. The Executive Leadership Team ('ELT'), and ultimately the directors, ensure that these risks are managed, maintained, reviewed and mitigated according to these frameworks. The Group's Internal Audit function continues to provide assurance over the effectiveness of mitigating controls. While copies of these reports are provided to the ELT to action any necessary control improvements, the Internal Audit function reports directly to the Audit Committee who monitor and challenge management to ensure control improvements are actioned.

The diagram below summarises the approach and responsibilities for the year.

Risk Management Framework

Board of Directors

Overall responsibility for maintaining sound risk management and internal controls. Assess principal risks and set risk appetite. Approve the viability statement.

Audit Committee

Set risk management framework. Assess effectiveness of the Group's risk framework and internal controls, including direction of internal audit.

Executive Leadership Team

Implement risk management framework. Assess effectiveness of the Group's risk framework and internal controls

Risk & Controls and Internal Audit

Test internal controls and co-ordinate risk management activity, provide support to business risk owners and report risk information across the Group.

Operational Management

Own and review operational risks, operate controls and implement mitigation actions. Escalate concerns regarding emerging risks or changes to existing risks.



During the year, we enhanced our enterprise risk management process. This included comprehensively updating the Group's Risk Policy that was reviewed and approved by the Audit Committee, as well as redefining our risk taxonomy, and updating the risk register framework to capture and consider more attributes associated with our key risks.

The ELT lead the refreshed risk identification process, which included each member of the ELT holding an extended workshop with their functional leadership teams to consider the full population of risks considered relevant to their areas of responsibility and the Company as a whole. This was followed by a robust ELT-level review of identified

risks, their categorisation, and relevant mitigating actions. In addition, an extended workshop was held with the non-executive directors to share the enhanced process being used by the Group and obtain their input given their broad experience. The combined output was then reviewed by the whole Board.

The process is summarised below.



For FY25/26, we will conduct further workshops, and the periodic ELT reviews will continue to ensure we identify emerging risks and to monitor the effectiveness of the controls that mitigate our key risks. In addition, a Risk and Controls management committee will be in place, with representation from risk owners from senior management risk owners, the Risk & Controls and Internal Audit functions, and key ELT members.

Output from the Group's risk management process will continue to be reviewed by the Board and the Audit Committee in line with the responsibilities of the UK Corporate Governance Code.

Principal risks and uncertainties

The Board has conducted a robust assessment of the principal and emerging risks facing the Group. These are based on the most critical individual risks on our refreshed risk register, some of which have been aggregated. They include those that we consider could most impact our business model (see pages 03 to 05), the delivery of our long-term strategic objectives (see pages 08 and 09), and that could threaten our future performance, solvency or liquidity. These risks and uncertainties (pre-mitigation) are set out in this report, together with a description including key mitigating activities in place to address them.

The 'Changes in FY24/25' information for each principal risk highlights changes in the profile of our principal risks and/or describe our experience and activity over the last year.

As a result of our risk management refresh programme, we have updated certain of our principal risks.

- 'Technology' has been renamed as 'Technology and cyber'.
- 'HR and employee' risk is now 'People'.
- 'Food safety' continues to be of pivotal importance. It is now shown as a separate principal risk, having previously been subsumed in 'Operational integrity'.
- 'Strategic delivery' has been removed. Our review programme identifies all key risks against the five strategy pillars and the most significant, either individually or in aggregate, form the principal risks. These risks – and how we manage them – are therefore the underlying factors that may impact delivery of our strategy.
- Consequently, we also now include 'M&A activity' as a separate principal risk relating directly to our strategy pillar of 'Inorganic opportunities'.

Risk appetite

Our approach is to minimise exposure to reputational, financial and operational risk while accepting and recognising a risk/reward trade-off in pursuit of our strategic and commercial objectives. We operate in a challenging and highly competitive marketplace, and, as a result, we recognise that strategic, commercial and investment risks will be required to seize opportunities and deliver results. We are therefore prepared to make certain financial and operational investments in pursuit of growth objectives. Our acceptance of risk is subject to ensuring that potential benefits and risks are fully understood and appropriate measures to mitigate those risks are first established.

The principal risks for which we have least tolerance are those that could prevent us from ensuring that our products are safely made and delivered on time to our customers. That includes making sure that the supply chain from start to finish is not subject to large scale interruption, including that from a cyber-attack. As these significant risks could materialise rapidly, we prioritise mitigation of them.

Risk management

The Group has a risk management framework to identify, evaluate, mitigate and monitor the risks the business faces. The risk management framework incorporates both a top-down and a bottom-up approach to ensure all the Group's risks are identified.

During the year, the risk management process was enhanced. This included a new Enterprise Risk Management Policy, framework and taxonomy. Over the year the process has been run across all Group functions. Initial 'bottom up' reviews were being undertaken with ELT members and their leadership teams via workshops as part of the initial risk identification stage; current mitigation activities were also collated to form a baseline set of controls. In addition, a separate non-executive Risk Workshop, facilitated by the Director of Internal Audit and Risk, was held to provide a top-down assessment of material risks. Following this process, the Committee then carried out a review of the enhanced risk register and the resulting reported principal risks facing the business. The output from these assessments has, subsequently, been presented to and reviewed by the Board, who retain ultimate accountability for risk management for the Group, for further review and discussion.

Further details of our risk management process are set out in the 'Risk management' section of this Annual Report.

Internal controls

The Committee maintains responsibility for reviewing the process for identifying and managing risk and for reviewing internal controls. It receives reports from management, the Director of Internal Audit and Risk, and the statutory auditors, in addition to the results of any investigations performed as a result of colleague whistleblowing reports, or otherwise. The Committee considers the implications of findings from the risk management process and from both the internal and external auditors to the Group's controls framework. Any issues are reported and discussed, and management are challenged as to what actions they are taking to improve the control framework and minimise the likelihood of their reoccurrence.

The Board has delegated authority to the Committee to monitor internal controls and conduct the annual review. This review covers all material controls, such as financial, operational and compliance, the preparation of the Group's consolidated financial statements, and also the overall risk management system in place throughout the year under review, up to the date of this Annual Report. The Committee reports the results of this review to the Board for discussion and, when necessary, agreement on the actions required to address any material control weaknesses. The Committee confirms that it has not been advised of any failures of material controls or material control weaknesses during the year and the Committee concluded that the Group's internal controls framework remains effective.

During the year, the Committee continued to receive updates on the Group's preparations for the enhanced risk and control disclosures required by the FRC's UK Corporate Governance Code 2024, to ensure that the Group meets its responsibilities. A Steering Committee, chaired by the CFO, oversees a Project Execution Team. The testing programme is now in its second year and supported by the introduction of a new integrated risk management and controls platform to provide a central repository for documentation, controls testing and self-assessments. As at period-end, all controls tested were deemed effective and the overall control framework was deemed to be operating effectively.

Source: https://www.premierfoods.co.uk/wp-content/uploads/2025/06/Premier-Foods-Annual-Report-2025.pdf?_gl=1*8ozvoz*_up*MQ..*_ga*MTcwMTA2MTI5LjE3NDg5NDg4MTU.*_ga_6RBRHP33EG*cze3NDg5NDg4MTQkbzEkZzAkDE3NDg5NDg4NDYkajl4JGwwJGgw

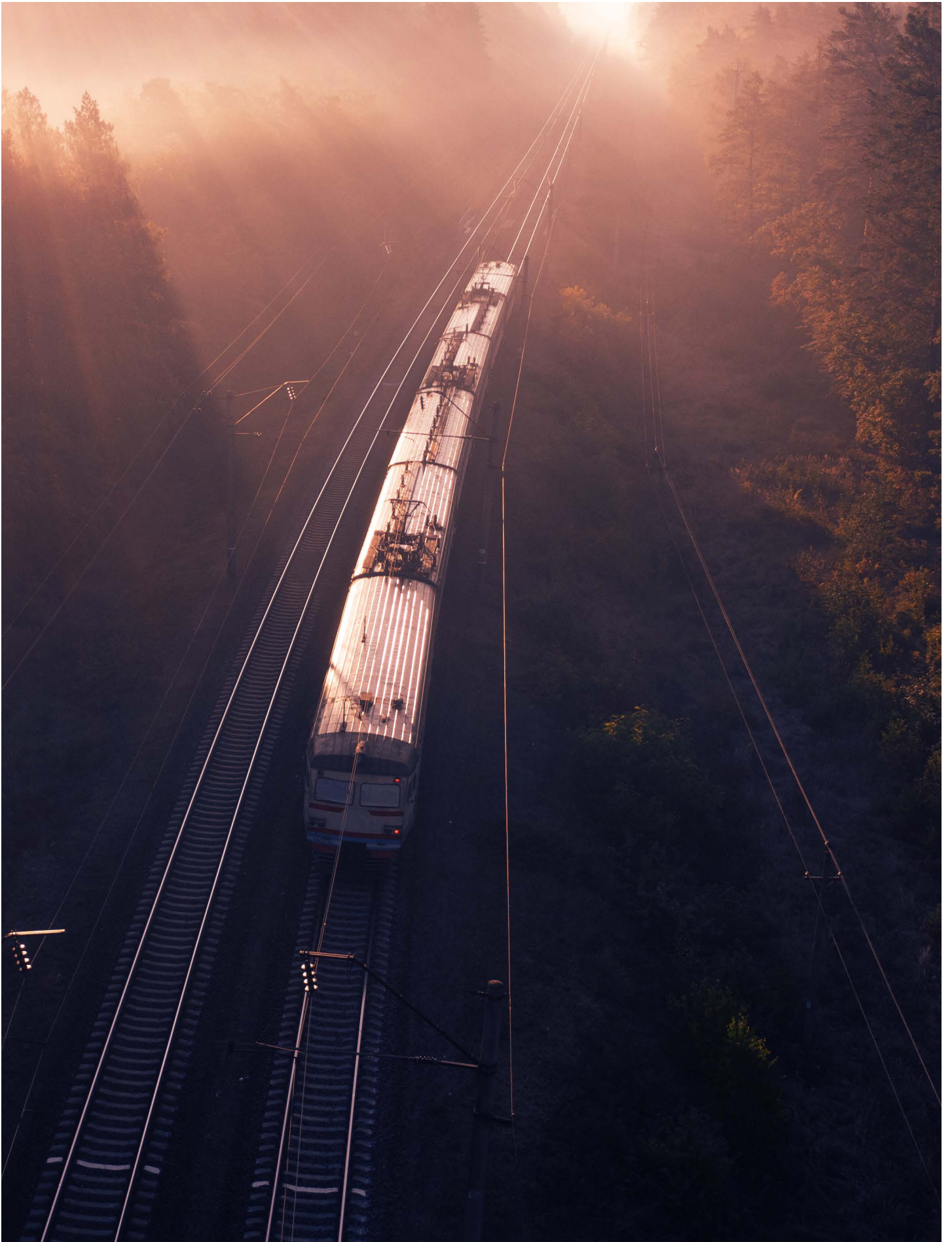


Figure 6

Rolls-Royce 2024 ARA, p. 52-53

Principal risks

The Rolls-Royce risk management and internal control framework

Taking risks is an essential part of running a robust, profitable business. Effective risk management helps us to identify anything that could hinder or support the effective implementation of our strategy and business model, then take action to address it. In order to achieve this, we have an established risk management and control framework, shown in the diagram below.

Our framework aligns with international standards for managing risk and sets out requirements across the Group for all risk categories. This includes climate, finance, legal, operations, technical and programmes, as well as providing guidance, training and tools.

The Board is ultimately responsible for our approach to risk management and internal controls. In February 2024, it endorsed the framework in operation for that year, monitoring its effectiveness by assessing:

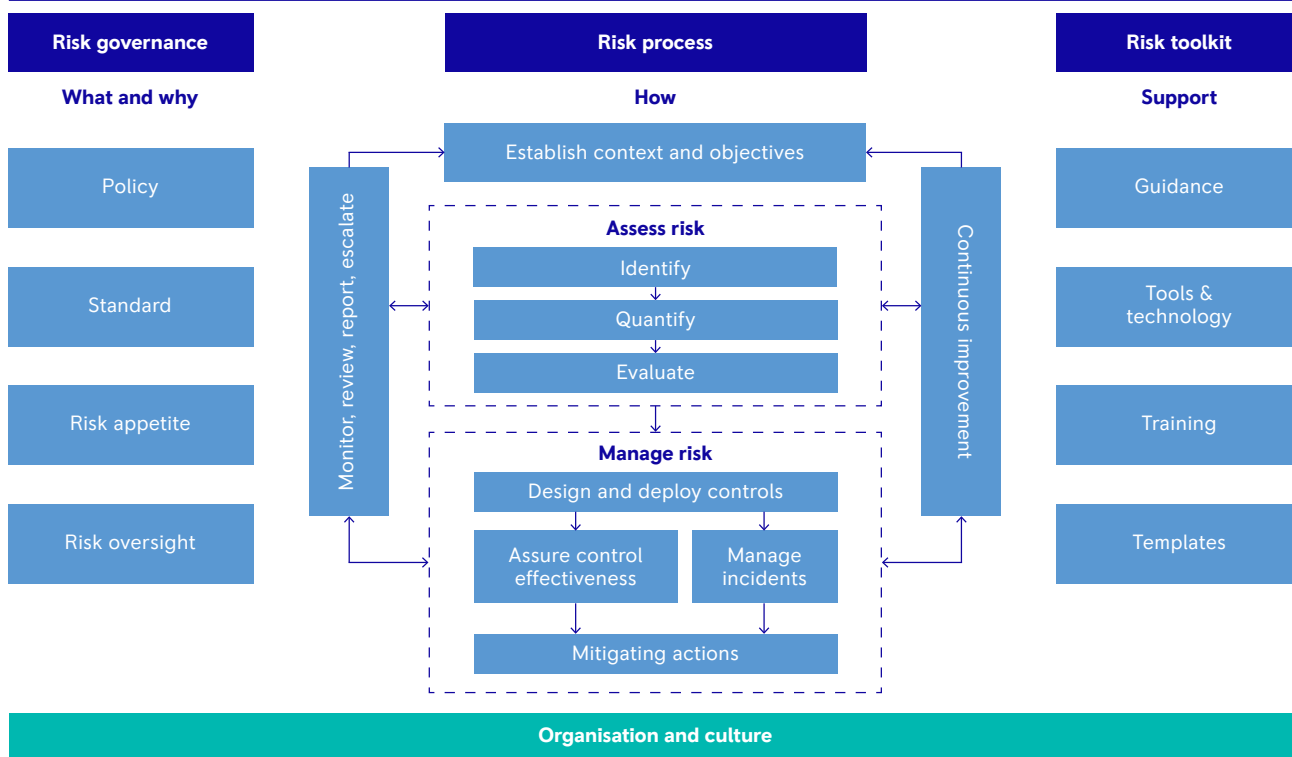
1. How effective the framework was at managing the principal risks:
 - Individual principal risks with reports throughout the year at the appropriate Board Committee, led by the risk owner (with a focus on controls in place to manage the risk and mitigating actions required to close any gaps). See pages 75 to 76 for a detailed list of these reviews.

- A report by the head of enterprise risk management covering the principal risk portfolio to consider the current overall risk levels compared to risk appetite and our own internal targets.
2. The Group's internal financial controls (at the Audit Committee) with financial reporting controls being subject to periodic review by the Group's internal controls team.
 3. The effectiveness of the framework more broadly at improving the risk culture and capability of the organisation, including an annual risk maturity assessment.
 4. The input from assurance providers, such as the internal audit team, where risk-related findings are taken into account in managing related risks.

See page 53 for more on progress in 2024 and future risk improvement plans, as well as page 84 for more information on internal audit.

The Board confirms that it has monitored the effectiveness of risk management and internal controls throughout the year, in accordance with the Code.

The risk management framework



How Rolls-Royce uses the framework to manage risk

Risk governance

Risk governance sets out the roles and responsibilities, as well as the why and the what, of risk management. Clearly outlining our approach to risk oversight enables the Board and Executive Team to receive the risk information it needs to consider: the nature of our principal risks (individually and as a portfolio); their current and target risk levels, including whether or not they are within our risk appetite; the extent to which mitigation is effective; and the status of associated improvement actions. In addition to the Board oversight outlined on pages 74 to 75, the Executive Team reviews individual and portfolio principal risk reports, with the latter (with the addition of divisional level risk information), being considered as an input into the five-year planning process. These reports contain the current risks, their status, controls information and action plans to remediate any gaps.

Risk process

We use the framework to set expectations across the Group on the steps to follow when managing and talking about risks:

Identify	Risks can be identified by anyone across the Group, including emerging risks as well as what could stop us achieving our strategic, operational or compliance objectives or impact the sustainability of our business model (described on pages 14 and 15).
Quantify and evaluate	Risk owners quantify the likelihood of a risk materialising and the potential impact if it does, taking into account current effective controls, and then deciding on a plan of action.
Control and assure	Risk owners design, implement and assure the effectiveness of controls to manage the risk, supported by different assurance providers using a three lines of defence approach (detailed in the principal risk tables from pages 55 to 60).
Act	Risk owners identify where mitigating actions are needed to bring the risk within appetite, assessing the Group's ability to reduce the impact of risks that materialise and ensuring the costs of operating a control are proportionate to the benefit provided.
Monitor, review and report	Risk owners report their assessment of current and target risk scores to local leadership as well as other review forums (including the Board and its Committees and the Executive Team) as needed depending on the level of the risk, for support, challenge and oversight.

Risk toolkit

The above are underpinned by a toolkit of guidance, templates, tools and training. For some principal risks, such as safety and compliance, there are mandatory training and policies in place, linked to performance management and remuneration, which all our people are required to complete and comply with (see page 47 for details).

The framework rests on the appropriate organisation and culture, with individuals at all levels (starting with the Executive Team) demonstrating the principles of good risk management and the capabilities to deliver on these. An independent enterprise risk management team supports the divisions and functions in their effective management of risk.

Risk maturity and continuous improvement

We continually look for ways to improve how we manage risks, such as action planning to bring a risk level down or developing training to support risk owners. We also ensure the framework itself is fit for purpose through regular benchmarking against best practice risk standards as well as active participation in industry groups.

Improvements in 2024

Following the implementation of the new risk framework and oversight approach in February and the implementation of a new organisational design, we have increasing confidence in the assessment of our risks, with a real focus on mitigating actions to get to an agreed target risk level, as well as more transparent reporting. We have also seen a positive shift in the risk culture of the organisation, with strong risk awareness and engagement.

The new framework places even more emphasis on the importance of controls and assurance in managing risks well and our risk, controls and assurance (RCA) programme has continued to support the design and documentation of controls for principal risks, embedding these controls in our management system.

2025 and beyond

Plans are now in place to ensure our readiness to meet the additional reporting requirements of the 2024 UK Corporate Governance Code. The RCA programme is a key foundational activity in relation to principal risks and, as such, will form part of the integrated Group-wide plan, which also incorporates other areas such as financial and non-financial reporting (including sustainability reporting requirements) and compliance.

We will maintain focus on completing agreed actions to continue to mitigate our principal risks within appetite and on assuring the effectiveness of our internal controls.

Source: <https://www.rolls-royce.com/~media/Files/R/Rolls-Royce/documents/annual-report/2025/2024-annual-report.pdf>

Figure 7

JTC 2024 ARA, p. 61, 65

Risk Management Framework

The Group Risk Management Framework is designed to ensure that risks are managed and controlled effectively across all operations and functions.

The PLC Board and senior management are responsible for setting organisational goals, establishing strategies to achieve them, and establishing governance, risk management and control frameworks to manage risks and achieve these objectives.

The Governance and Risk Committee of the PLC Board consisting of the PLC Non-Executive Directors operates to assist the Board in complying with corporate governance regulations and codes, assessing the Group's attitude to and appetite for risk, oversight of the Group's systems of internal control and risk management, compliance with laws and regulations and how risk is reported.

The Group applies a risk taxonomy that aligns the risks faced by JTC across eight high level (Level 1) categories which are further sub-divided into 34 (Level 2) risk descriptions.

The GRC is a sub-committee of the Group Holdings Board (GHB) and comprises the Group Chief Executive, Chief Risk Officer, Group General Counsel and Group Director – Risk & Compliance and is also attended by the Group Divisional Heads. The GRC meets monthly to monitor emerging trends and risks, assess the effectiveness of systems and controls, and consider risk matters of significance that may materially impact the Group and require strategic direction and/or action.

The GRC will make recommendations to GHB and ultimately the PLC Board on risk matters including the identification of the Group's principal risks, material controls and their effectiveness, and the Group's approach to risk appetite.

During 2024, a refinement of the Group's risk taxonomy was approved to provide a more granular categorisation of risks increasing the number of Level 1 risk categories from six to eight. The promotion of Financial Crime and ESG risks to the higher Level 1 category ensured a more detailed approach to the Level 2 sub-risks and will allow greater alignment to the new GRC system mentioned above. These changes aim to support the Board in reporting on the effectiveness of the Group's material controls under enhancements to the UK Corporate Governance Code due to come into effect in 2026.

The change to the taxonomy also necessitated an update to the Group's Risk Appetite Statement described on the following page.

Level 1 Primary, overarching risk elements, containing eight components	Level 2 Represents the cohorts of specific risks JTC is exposed to	Principal Risk	Strategic Risk	Political & Regulatory Risk
1. Strategic	Acquisition	●	1 Acquisition	7 Compliance
	Competitor and client demand ¹		2 Strategy & Culture	Financial Crime
	Strategy & culture ²	●	Financial	8 AML/CFT/CPF Risk Assessment
2. Financial	Performance of business	●	3 Performance of Business	Legal Risk
	Earnings (FX)		4 Reporting	9 Fiduciary
	Impairment		Operational Risk	Human Resources Risk
	Financing		5 Client	10 Adequate Resources
	Reporting ³	●	6 Technology/Data Security	
	Capital adequacy			
3. Operational	Client ⁴	●		
	Process ⁴			
	Resilience & Business Continuity			
	Technology/Data Security ⁵	●		
4. Political/Regulatory	Listing rules			
	Political			
	Regulatory			
	Compliance ⁶	●		
5. Financial Crime ⁷	AML/CFT/CPF Risk Assessment ⁷	●		
	Organisational			
	Countries, Territories or Geographic Areas			
	Customer			
	Customer Due Diligence			
	Delivery Channels			
	Products, Services and Transactions			
	Fraud			
	Anti-Bribery & Corruption			
6. Legal	Litigation/Contractual			
	Fiduciary	●		
7. Human Resources	Adequate resources	●		
	Remuneration & Incentivisation			
	Key Person			
8. ESG ⁸	Environmental			
	Social			
	Governance			

Notes – 2024 changes and updates to principal risks

- 1 Removed as a principal risk due to business growth success and low regretted attrition reducing impact of this risk category.
- 2 Risk description expanded to also reference culture.
- 3 New principal risk to reflect the increasing complexity in reporting consolidated financial information across multiple jurisdictions and legal entities.
- 4 Separation of risk categories to ensure a more focussed approach to the principal risk associated with client relationships.
- 5 Risk description expanded to also reference Technology risk acknowledging the full spectrum of risks relating to IT failure or compromise.
- 6 Renamed to Compliance (from Political/Regulation) to focus upon the principal risk relating to adherence to law, regulations and policies.
- 7 Promotion of Financial Crime from a Level 2 category to Level 1 to allow a more granular assessment of financial crime risk and allow focus on the principal risk in assessing anti-money laundering and countering terrorist and proliferation financing risk.
- 8 New Level 1 risks to recognise the increasing significance of ESG matters to commercial enterprises.

Source: https://annual-report.jtcgroup.com/.2024/publication/contents/templates/JTC_Group_annual_report_2024.pdf

Figure 8

Derwent 2024 ARA, p. 149

Effectiveness of material controls

Following the publication of the UK Corporate Governance Code 2024, preparations are well underway to ensure compliance with the requirements of provision 29 for the year ending 31 December 2026. A timeline outlining the key milestones to achieving compliance is outlined below.

Our approach

An initial proposal on material controls (financial and non-financial) and assurance has been reviewed by the Risk and Audit Committees and is subject to further enhancement in preparation for a 'dry run' in H2 2025.

Existing governance structures mean that the Board and its principal committees already report upon the effectiveness of a range of controls in the annual Report & Accounts. Efforts are therefore being focused on leveraging this strong foundation and strengthening any gaps to ensure the Board has the requisite level of confidence in making their annual declaration on the effectiveness of material controls.

Identifying our material controls

Materiality for the purposes of complying with provision 29 of the Code has been informed by looking at Derwent London's risk appetite, Schedule of Principal Risks, Board Assurance Framework as well as detailed risk assessments and controls documentation. It takes into consideration the size, nature and complexity of our operations as well as the requirements of various reporting regimes, laws and regulations that we are obliged to comply with.

We have defined our material controls as those that are most important in mitigating key risks that threaten the long-term sustainability of the business, and where a failure of their effective operation, or a resulting omission and/or misstatement of information caused by the control failure is likely to influence decisions made by users of the information. They have been grouped into six categories as set out in the diagram below.



Assurance

While the Code does not require independent or external assurance to be obtained, for those material controls that have the highest impact of the long-term sustainability of the organisation and are most likely to influence decision makers, independent/external assurance will be sought in line with good practice.

To date, existing assurance activities have been mapped against proposed material controls using the Board Assurance Framework and knowledge of the assurance environment. An assessment of the strength of current assurance activities has been performed, and where gaps have been identified, recommendations for additional assurance have been made for consideration by the Board.

Key milestones to compliance

January 2024	FRC published the UK Corporate Governance Code 2024 and supporting guidance
August 2024	Schedule of Principal Risks was rationalised
November 2024	Draft material controls and assurance proposal reviewed by the Risk and Audit Committees
H1 2025	Revised material controls to be reviewed and agreed in principle by the Audit and Risk Committees and the Board
H2 2025	A 'dry run' of material controls assurance pack to be reviewed by the Audit Committee and adjustments made as required
H1 & H2 2026	Updates on assurance outcomes performed throughout the year provided to the Audit Committee
H2 2026	Material controls assurance pack to be reviewed by the Audit Committee
December 2026	Annual Report & Accounts for year ending 31 December 2026 to include the Board's declaration on the effectiveness of material controls

Completed In progress To be completed

Source: <https://www.derwentlondon.com/uploads/downloads/Annual-Report-Accounts-2024-single-page.pdf>

Figure 9

Drax 2024 ARA, p. 72, 116-117

Risk management governance

The Group's risk management governance structure includes the Executive Committee and various other risk management committees covering each of the Group's Principal Risks. The committees have responsibility for:

- Assessing and understanding the risks that may impact our business to ensure any new, current or emerging risks are managed within the defined risk appetite and limits of the business
- Reviewing changes in the internal business and external macro environment and responding appropriately
- Driving completion of the actions required to improve the mitigation of risks and where possible reduce risk exposures to target levels
- Enabling an appropriate risk management culture that promotes and creates balanced risk-taking behaviour and clear accountability

Risk management committees at the business unit and Group function level undertake risk reviews on a rotational basis, receiving reports from subject matter specialists and risk owners to inform these reviews where appropriate.

The Executive Committee (from which owners are identified as accountable for each Principal Risk) undertakes deep-dive reviews of each Principal Risk through an annual cycle and receives ad-hoc reports from the risk management committees and Principal Risk owners as required. Please refer to the Audit Committee report on page 112 to understand how the Audit Committee oversees the Group's Principal Risks.

Review of effectiveness

The Board is responsible for determining risk appetite and ensuring the effectiveness of risk management and internal controls across the Group.

A quarterly update is provided at each meeting of the Audit Committee. More information about the Audit Committee's process of review and resulting findings can be found on pages 112 to 125. During 2024, enhancements to risk management included the strengthening of the Sustainability Council; providing independent governance and oversight from stakeholders across the business; ongoing alignment of second line IT testing with best practice auditing standards; and the continuing roll-out of an enhanced Group-wide compliance framework to ensure that consistent, risk-based controls and governance are embedded across all areas of the business responsible for external compliance obligations. This work forms part of an ongoing Compliance Action Plan. To date work has been completed to collate a register of the Group's compliance obligations, undertake respective risk assessments and establish a self-assessment of the current levels of control and governance that support them.

The review of the effectiveness of the Company's risk management and internal control systems is undertaken by the Audit Committee and reviewed against FRC guidance and any significant gaps are highlighted to the Board. There were no instances in 2024 where management identified gaps in risk management or internal control that would have had a material impact on the Group's operational

performance, financial performance or results. As such, the Committee was satisfied that risk management and control systems continue to operate effectively in all material respects.

The Committee's review is supported by the quarterly Risk and Control update provided by management to the Committee. These updates detail any material changes in the Group's Principal Risks and the associated controls employed to manage them. It also summarises the outcome of management's process of self-attestations and second line sample testing of key internal controls, as well as other instances where significant weaknesses in internal control have been identified. Finally, updates are provided on the findings from the internal audit plan, which is approved by the Audit Committee for each forthcoming year in December, and progress on implementing any resulting actions is reported to the Committee at each subsequent meeting. Taken together, the Audit Committee forms a view on the overall effectiveness of the systems of risk management and internal control.

The Audit Committee and Board consider and challenge on the culture and behaviours to risk management which are important factors in establishing and operating effective response to risks facing the Group. This is supported by the combination of business-led reviews of risk, the contribution of risk committees and the use of an external internal audit function that evaluates managements approach.



Rob Shuter
Audit Committee Chair

The Committee regularly reviews and considers the effectiveness of the Group's internal controls, assessing risks and mitigation activities, and monitoring their potential impact on the Group's strategy and viability. This includes assessment of emerging risks, particularly as the Group expands operationally and geographically.

You can read more about the Audit Committee's activities on pages 112 to 125

Audit Committee report

Reviewing the effectiveness of the system of risk management and internal controls

Alongside the expert support provided by the Group's internal auditor, management is required to perform a regular self-assessment and review of risk management and internal control activities covering the Group's Principal Risks.

Control owners provide an assessment on the operation of key controls at least twice annually, and report on any gaps or control failures identified. These responses are then reviewed by the second line Group Risk team, and the assessments of control operation and effectiveness are periodically challenged and validated to supporting evidence. The outputs from the assessment are reported to the Committee at each meeting. At the meeting held in December 2024, this included communication of the fact that incomplete or inaccurate supplier data was in some instances delaying due diligence procedures. It was agreed that resource should be dedicated to remediate this control ineffectiveness as a priority.

The second line review is undertaken in the context of broader changes in both the underlying risks and the environment in which the Group is operating, and considers whether prevailing controls remain appropriate and sufficient. To support this, the Committee annually reviews a detailed assurance map for the Group, covering each of the Principal Risks. The assurance map summarises the controls and assurance in place across the different lines of defence, as outlined on page 71. It also provides management's assessment of whether the level of control and assurance is appropriate, and highlights ongoing work to address any opportunities for enhancement.

Having reviewed the latest assurance map at its meeting in December 2024, the Committee was satisfied that there were no significant gaps in the levels of assurance. Progress made during 2024 included the introduction of a Political Engagement Register and respective training for those authorised to undertake political engagement, enhancing prevailing practices and the establishment of a framework of key human resources-

related controls for self-assessment and verification to supporting evidence.

Changes to the Corporate Governance Code were announced in 2024, which will require Boards to make a declaration in relation to the effectiveness of material internal controls. This will apply to the Group from the financial year beginning 1 January 2026 onwards. In December 2024, management presented an updated roadmap to the Committee setting out the key actions required in advance of the first internal control declaration to be made in relation to the 2026 year end, and a proposed definition of 'material' to be applied in identifying which controls fall into the scope of the declaration.

The 'business as usual' operating model for maintaining and governing the Group's framework of material controls beyond 31 December 2026 was also presented to the Committee along with a proposed plan of internal and external assurance to be obtained over the design and operation of the Group's material controls.

Progress against this roadmap during 2024 was discussed with the Committee, including the formalisation of a library of Entity Level Controls and an initial mapping exercise of those controls considered to be material to the Group's operations, compliance, and reporting. The key milestones to be achieved during 2025 were also considered by the Committee, including an initial dry run of assurance intended to support the internal control declaration, the development of a controls policy, and further training of control owners.

Following its review, the Committee approved the proposed materiality definition and agreed with management's plans and the proposed levels of assurance. It was confirmed that quarterly updates would continue to be provided to the Committee on the progress made and any divergence from the roadmap.

Source: https://www.drax.com/wp-content/uploads/2025/05/Drax_AR2024_Interactive.pdf



Figure 10

JD Sports Fashion FY25 ARA, p. 44-45, 106-110

Principal Risks

OUR FRAMEWORK AND PROCESS

Risk Management Process

Our Risk Management Framework ('RMF') sets the foundations and arrangements for risk management across JD Sports Fashion Plc. The purpose of the framework is to assist the Board in executing the Group strategy by providing a standard approach and process for the management of risk. By clearly defining the Group approach to risk, it allows us to have a common language and set of standards to be applied, providing clarity in the information used for decision making. A common risk language means that management can more easily consider risk priorities across all divisions, fascias and processes, and thus can act on areas of greatest importance to the Group.

The RMF contains nine risk appetite statements which underpin our Key Risk Areas ('KRAs'). Each statement defines the level of risk which the Group is willing to accept in normal business operations, before taking additional action. Depending on our risk appetite, we either mitigate, accept, or take action to reduce. The Board is responsible for refreshing these statements on an annual basis and aligning with the Board's commitment to manage risk effectively. Further, the Board sees the value in a connected and embedded process where risks and opportunities are considered when making decisions to meet strategic objectives.

Key Risk Areas

During the year, the Plc Board and Audit & Risk Committee reviewed the KRAs for the Group. These are determined by reference to the sector and markets we operate in, our overall business model and our strategic aims. The nine KRAs below drive the overall structure of risk identification, assessment and management. Each KRA has an Executive owner, who has day-to-day responsibility for managing risks within the defined risk appetite, agreeing controls and mitigations, and Key Risk Indicators ('KRIs') to support monitoring and reporting. During the year, responsibility for merchandising has moved from Logistics to Retail Operations to better align with the Executive structure.

Key Risk Areas



Risk Management and Internal Controls

The Board, in conjunction with the Audit & Risk Committee, has full responsibility for monitoring the effectiveness of the Group's system of risk management and the supporting system of internal controls. Executive Directors and Senior Management, as part of the Executive Risk Committee, are tasked with managing risk on a day-to-day basis. Additionally, the Board operates the following features of risk management and internal controls:

- A well-defined organisational structure with clear roles and responsibilities.
- Ongoing roll-out of an Entity Levels Controls Framework, including a suite of policies and procedures. These are designed to communicate expectations and set standards in key areas such as Health & Safety, Information Security, Whistleblowing, Bribery Law and Competition law.
- Identification and monitoring of the business risks facing the Group, including: consideration of assurance sources and controls; and further assurance work as necessary, including investing in teams which focus on internal control, risk-based assurance and profit and asset protection.
- Detailed appraisal and authorisation procedures for commitments and investment, which are documented in the Matters Reserved for the Board, Delegated Levels of Authority document, and the Group's Contract Authorisation Policy.
- Preparation of monthly management accounts providing relevant, reliable and up-to-date information. These allow for comparison with budget and prior year results. Significant variances from approved budgets are investigated as appropriate.

- Preparation of annual budgets allowing management to monitor business activities, major risks and the progress towards financial objectives in the short and medium term.
- Monitoring of store procedures and the reporting and investigation of suspected fraudulent activities.
- Reconciliation and checking of all cash and stock balances and investigation of any material differences. The Board continues to review opportunities to develop, strengthen and optimise the effectiveness of these systems.

An experienced Group Head of Assurance has overseen both Internal Audit and Enterprise Risk Management capability during the year. Moving forward, we are separating the risk management function in line with a traditional three lines of defence model. An experienced Head of Risk will join the Group in Q2. The Board, via the Audit & Risk Committee has approved the RMF. As part of this framework, a quarterly Executive Risk Committee reviews and acts upon risk information.

The RMF provides a standardised basis for identifying, assessing and managing enterprise level risks. It also contains risk appetite statements which have been approved by the Board and are referenced within each KRA in further detail from page 46. These statements underpin the Board's commitment to managing risk effectively.

Continuous Improvement

The Group Risk team regularly consider the appropriateness of the RMF against best practice risk management standards and via active participation in external risk industry groups. Any proposed changes to the framework are presented to the Executive Risk Committee and Audit & Risk Committee for approval.

During the year, we have introduced a rolling programme of deep dives into risk topics at both the Executive Risk Committee and Audit and Risk Committee. At these sessions, the risk owners present to the governance forums on current and emerging threats, and activities taken to mitigate potential risks. During the year, Cyber and Data Protection risks have been considered in detail.

During the year, we have started the process to roll out the RMF to the wider business via a series of divisional risk workshops. These workshops are refining our view of risk and in time, we expect a similar routine of risk reviews and KRI reporting that we have now established at the Group level to operate divisionally.

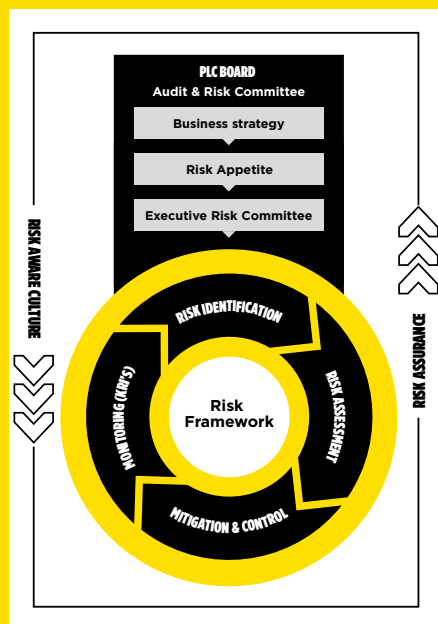
Internal Controls Programme

Our internal controls programme continues to progress, with a near-term focus on internal controls over financial reporting and IT controls. Our programme of work will also include planning assessment and reporting on Material Controls, as required by the updated Corporate Governance Code on Provision 29. Work of the Internal Controls team currently extends to the following:

- Group-wide internal controls over the financial reporting framework: Ensuring consistency, accuracy, and reliability in financial reporting across the organisation.
- Entity-level controls aligned to the COSO framework: These controls are being enhanced to ensure robustness and consistency of control across the Group.
- Assessment of the risk of material fraud: identifying potential sources of material fraud and confirming the presence of effective controls.
- Future developments in internal controls: identifying and evaluating material controls over reporting, operational and compliance risks to align with Provision 29.

The Board continues to support the development of Risk Management and Internal Control activities, in line with Group-wide improvement plans, as previously reported.

Refer to the Audit & Risk Committee Report on page 106 for the assessment of the effectiveness of internal controls.





Helen Ashton
Chair of the Audit & Risk Committee

Audit & Risk Committee members as at 1 February 2025	Meetings attended
Helen Ashton	6/6
Ian Dyson	6/6
Darren Shapland	6/6
Kath Smith	6/6

The last 12 months have seen continued progress in improving the Group's governance position under the stewardship of the Audit & Risk Committee.

Although we are only part way through a multi-year journey, we are encouraged by the ever evolving quality and commitment of the JD team which is leading the programme to deliver a control and risk environment that is appropriate and proportionate for the Group.

The FY26 priority areas for the Audit & Risk Committee are:

- preparing for enhanced disclosures under Provision 29;
- preparing for assurance of Corporate Sustainability Reporting Directive ('CSRD') metrics;
- continued oversight of the Finance Transformation programme focused on enhancing capability, systems and processes;
- embedding the Group Risk Management Framework including deep dives of the Group's key risks;
- continued build out of the Group Internal Audit function coupled with embedding the Group's three lines of defence; and
- oversight of the IT General Controls ('ITGC') programme.

Internal Controls

- Kept under review the adequacy and effectiveness of the Group's internal financial controls (that is, the systems established to identify, assess, manage and monitor financial risk) and risk management systems.
- Oversaw the Group's progress in improving the effectiveness of Internal Control over Financial Reporting ('ICFR') and IT General Controls ('ITGC'). Further information regarding ICFR is included in the Financial Reporting Controls section later in the report. Further information regarding ITGCs are covered in the IT General Control section later in this report.
- Considered reports from the External Auditor on progress and the results of the External Auditor's testing of controls as part of the External Auditor's work.
- Reviewed the adequacy and security of the Group's Speak Up policy arrangements whereby staff and contractors of the Group may, in confidence, raise concerns about possible improprieties in financial reporting or other matters, and monitored any incidences of reports made under the policy.
- Reviewed and approved the Group's tax strategy and tax policy.

Risk Management

- Reviewed and approved the Group Risk Management Framework.
- Oversaw changes to Key Risk Areas in the period, to better align to the Executive structure.
- Considered future plans and the roadmap for embedding Risk Management both at Group level and within Business Units.
- Reviewed the resourcing model for Risk Management and approved funding to develop our internal capability.
- Considered appropriate systems and tools to support the development of effective Risk Management processes.
- Reviewed progress against the Risk Management Framework and deep dives into the Group's key risks, including on cyber and data protection.
- Reviewed progress on compliance with Provision 29 and entity level controls.
- Reviewed and approved risk appetite statements for each of the Key Risk Areas.
- Considered the appropriateness of the identified principal risks and uncertainties (see pages 44 to 53).

Key Developments During the Year

JD Sports Fashion Plc has been on a journey of governance and controls improvements and, as highlighted in last year's report, this will be a multiyear journey. During the year, the Group has continued to make good progress, with the Audit & Risk Committee overseeing:

- the expansion of the Group Finance team in both size and experience to improve the efficiency of the reporting and audit cycle in FY25 and beyond, and consistency of accounting across the Group;
- continued delivery of new Group consolidation, lease accounting and treasury management finance systems, the benefits of which will be delivered in FY26;
- progress in addressing the prioritised deficiencies within the ICFR programme;
- the development of a prioritised programme to enhance IT General Controls;

Financial Reporting Controls

The Corporate Governance Transformation programme, which concluded at the end of FY24, handed over a number of ICFR open deficiencies for remediation into business-as-usual. During FY25, the Group adopted a phased sprint approach to remediate the ICFR deficiencies, with a focus on remediating critical, high and medium priority deficiencies, and substantial progress has been made in remediating these at the current period end. These sprints were supported by a robust governance framework, including Finance Risk Meetings and Regional ICFR Boards, to ensure effective ownership, oversight, prioritisation and resolution of identified deficiencies.

Additional highlights from the ICFR programme include the following:

- Governance Structures: Finance Risk Meetings chaired by the Group CFO, and Regional ICFR Boards chaired by Regional CFOs, are critical in driving progress on controls remediation, and monitoring the embedding of controls.
- Toolkit Roll-out: A Financial Controls Toolkit, aligned to the Group Risk Management Framework, describes the key financial reporting processes and the controls needed to manage reporting risks. A key benefit of the toolkit is its role in training colleagues on the operation of controls, ensuring consistency in application and serving as a useful resource for onboarding new staff. The toolkit forms the foundation for further roll-out to all Business Units, standardising control practices across the Group.
- Sustainable Operation of Controls: A key focus has been ensuring the sustainable operation of remediated controls.
- Processes have been established to monitor ongoing control effectiveness through monthly confirmations from control owners and regular reviews at Finance Risk Meetings.

Timelines and Next Steps; FY26 Focus:

- Extending the ICFR framework to cover all Group entities, including those currently outside the scope of the initial programme and newly acquired businesses. The entities currently in the ICFR scope cover 89% of Group Revenue. The original scope of ICFR entities was determined through a materiality assessment of the FY22 results.
- Launching second-line assurance activities to independently validate the operation of controls and provide recommendations for control environment improvements.
- Embedding training initiatives to strengthen the accountability and awareness of control operations across the finance function.

While significant progress has been made, certain areas, particularly IT-related deficiencies, require further remediation before full reliance on remediated business controls can be achieved.

- the development and embedding of Regional ICFR Boards, chaired by Regional CFOs, to drive progress on controls remediation, and embed the operation of controls across the business;
- the roll-out of the Risk Management Framework to the wider business, via a series of divisional risk workshops, and Group key risk deep dives at the Audit & Risk Committee; and
- accelerated expansion of the Internal Audit function to deliver an appropriately broad Internal Audit programme.

Assessment of the Effectiveness of the Group's System of Internal Controls and Risk Management

Risk Management

As outlined on page 44, the Group has established a framework for risk management and continues to embed it across our operations. The Board, in conjunction with management, is responsible for determining risk appetite and managing risk mitigation. The Audit & Risk Committee has delegated authority to monitor and evaluate the effectiveness of the internal controls relied on for risk mitigation.

IT General Controls

In FY25, we turned our attention to the wider IT General Control environment.

Therefore, during the year, the Group has invested and established a structured remediation programme, led by the new Chief Technology & Transformation Officer ('CTTO') and a newly appointed Chief Information Security Officer to drive progress and address key deficiencies. This programme focuses on five core workstreams:

- 1 Information Technology Governance, Risk and Compliance ('IT GRC'): Establishing policies, standards and frameworks to strengthen IT governance and ensure alignment with regulatory and business requirements.
- 2 Identity and Access Management ('IAM'): Enhancing controls over system access to ensure that only authorised individuals can access systems and data required for their role.
- 3 Resilience and Recovery: Improving the Group's ability to recover IT operations in the event of IT or cyber incidents.
- 4 IT Change Management: Ensuring that changes to systems are appropriately managed, authorised and monitored to minimise disruption and risks.
- 5 Quick Wins and Tactical Remediation: Implementing targeted fixes to address the most critical deficiencies while laying the groundwork for longer-term improvements.

Timelines and Next Steps; FY26 Focus:

- Remediation of critical ITGCs: Prioritising the resolution of deficiencies that directly impact financial reporting.
- Strengthening governance: Improving programme governance to provide oversight, ensure alignment with strategic objectives, and monitor progress effectively.
- Deployment of foundational IAM capabilities: Deploying tools to improve privileged access management, focusing on systems critical to financial processes.
- Establishing a solid governance and Risk Management Framework: Finalising policies and governance frameworks to ensure ITGCs are standardised, consistent and applied group wide.

Management remains committed to addressing ITGC deficiencies and embedding sustainable controls across the Group. Progress updates will be regularly reviewed by the Audit & Risk Committee to monitor progress and ensure accountability and transparency.

Provision 29 Readiness and Non-Financial Controls

For listed companies with financial years starting on or after 1 January 2026, Provision 29 in the 2024 UK Corporate Governance Code comes into effect. Provision 29 considerably expands the disclosures companies need to make in their Annual Report on internal controls. From FY27 onwards, the Directors of the Company must comply (or explain) with Provision 29 in the following ways:

- Making a declaration in the Annual Report on the effectiveness of material controls at the balance sheet date. Provision 29 determines material controls to cover financial, reporting, compliance and operational controls.
- Describing any material controls that have not operated effectively, along with actions (taken or planned) to improve them.

The Group will comply with Provision 29 or will provide a cogent explanation where this is not possible. Management is taking a risk-based approach, aligned to the Group's Risk Management Framework.

Key steps completed on the Group's readiness for Provision 29:

- **Aligned Approach:** Management has an aligned approach, linking material controls to the Group's highest rated risks, per the Group Risk Management Framework.
- **Assurance Framework:** Development of an embedded assurance framework to provide the Board with confidence on the effectiveness of controls.
- **Dry-Run Evaluation:** A pilot disclosure process is planned for FY26 to test readiness ahead of the FY27 compliance deadline.

The Provision 29 readiness work above is supported by initiatives to enhance non-financial controls, including the following:

- **Entity-Level Controls ('ELCs'):** In FY25, the Group continued its work to refine and assess the design of ELCs, focusing on alignment with the COSO framework and ensuring these controls effectively support governance and risk management objectives. Action plans are in place to strengthen areas identified for improvement, and progress is being closely monitored by the Executive Risk Committee. The assessment of ELC operational effectiveness will form part of the Group's ongoing Provision 29 compliance efforts.
- **Cyber Security:** Continued evaluation of lessons learned from cyber incidents.
- **Fraud Risk Assessment:** The FY24 assessment has been updated to ensure compliance with the Economic Crime and Corporate Transparency Act. Identified gaps are in the process of being remediated.

Assessment Conclusions and Next Steps

The Committee acknowledges that, while progress has been made in enhancing the Group's control environment, the journey to maturity continues. For FY26, priority areas include:

- monitoring ongoing roll-out and embedding of IT General Controls sustainably across the Group;
- completing roll-out and embedding of the new Group reporting systems within the Finance Transformation programme;
- preparing for enhanced disclosures under Provision 29, including piloting the required attestation framework;
- reviewing reports of second-line testing on financial controls to evaluate their design and operational effectiveness;
- further embedding of Risk Management Framework and deep dives into the Group's key risks; and
- continuing to build the Group Internal Audit function.

The Group remains committed to building a robust internal control framework to support long-term strategic objectives.

Figure 11

Barclays 2024 ARA, p. 259, 265

The Health and Safety Risk Management Framework overview is as follows:

Health and Safety Forum			
Leadership	Statement of Commitment for Health and Safety		
H&S Data	Data: Performance against commitment		
Horizontal	Premises	People	Physical Security
Risks	Harm to people through physical injury arising from Barclays' activities (excluding Physical Security incidents)	Harm to colleagues as a result of health and wellbeing related hazard mismanagement L3	Physical security incidents resulting in harm to staff or external parties L3
Policies	Premises – Property and Health & Safety Policy	Health Services & Wellbeing Policy	Physical Security Policy
Standards	Premises – Health & Safety Standard	Health Services & Wellbeing Standard	Physical Security Standard

The ERMF is complemented by frameworks, policies and standards which are mainly aligned to individual principal risks:

- frameworks cover high level principles guiding the management of principal risks, and set out details of which policies are needed, and high level governance arrangements
- policies set out the control objectives and high level requirements to address the key principles articulated in their associated frameworks. Policies state 'what' those within scope are required to do
- standards set out the detail of the control requirements to ensure the control objectives set by the policies are met.

Policy and Standard

Barclays has a suite of health and safety (H&S) policies and standards, which include clear roles and responsibilities for leadership and colleagues. These combine under a single high-level statement of commitment endorsed by the Group Exco.

Health and Safety Management System

Barclays has implemented and maintains a comprehensive H&S management system globally, which is certified to the international standard ISO45001 in the USA, UK, India, Singapore, Hong Kong and Japan.

Health and Safety Risk Assessment and Assurance

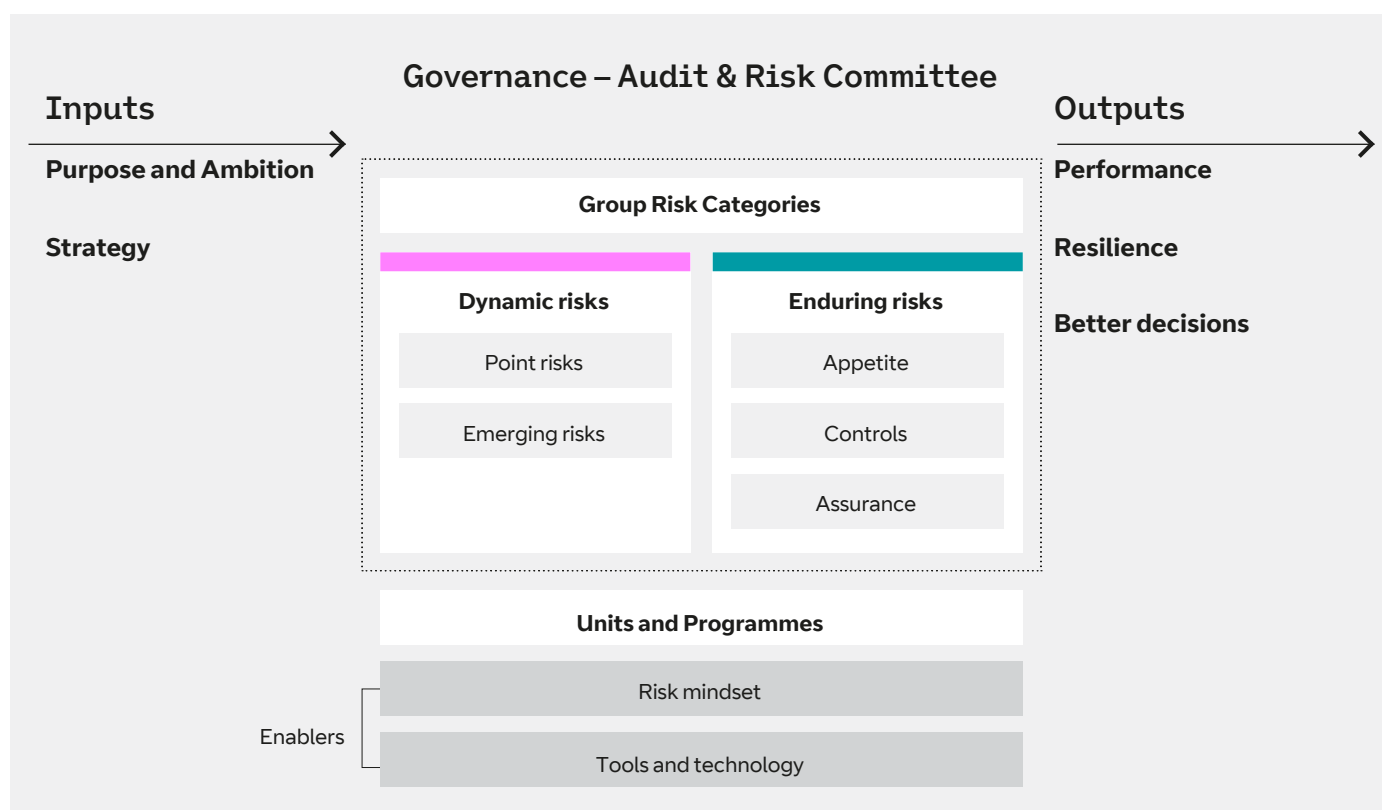
Barclays H&S management system is validated through H&S assurance and risk assessment programmes. Risk assessments identify hazards and the control measures required to proportionately manage the associated risks, whilst H&S assurance validates that control measures are designed effectively, implemented and operating effectively, and that site monitoring is taking place.

While H&S legislative requirements vary globally, our assurance and risk assessment programmes apply a risk-based approach, designed by our internal H&S team and informed by their experience, specific legislative requirements and relevant factors such as building type, building criticality, activities, and occupancy.

Source: <https://home.barclays/content/dam/home-barclays/documents/investor-relations/reports-and-events/annual-reports/2024/Barclays-PLC-Annual-Report-2024.pdf>

Figure 12

BT FY25 ARA, p. 54-55



How we manage risks

We divide our risk landscape into Group Risk Categories (GRCs). Each one has an *Executive Committee* sponsor accountable for applying the framework to that category.

Within each GRC we distinguish between enduring and dynamic risks.

Enduring risks need consistent, long-term structures to manage them – a clear risk appetite position, controls and assurance.

These structures then free us up to think about dynamic risks that need focused and timely responses: How big are they? Who do they impact? What do we need to do about them?

Dynamic risks are either:

1. Point: Risks potentially materially significant to us at a particular point in time that we can't manage within our existing control framework and which need focused attention.
2. Emerging: New and/or often longer-term risks with the potential to be materially significant that we can't fully define today.

You'll find the current status of the enduring and dynamic risks across our top 12 GRCs in the 'Our principal risks and uncertainties' section (see page 56) .

Figure 13

Vistry 2024 ARA, p. 120

INTERNAL AUDIT

The internal audit function's role is to systematically, independently and objectively assess the adequacy and effectiveness of the risk management systems and key internal controls over the Group's operations, financial reporting, IT systems, and risk and compliance processes. The function is a critical component of the Group's corporate governance framework providing support and assurance to the Board, Committee and management in the execution of the Group's strategy. It provides recommendations to address key issues identified and improve processes and controls and delivers important insight on issues of culture and employee values and behaviours.

The internal audit team has a blend of experience consisting of core expertise in risk and assurance, alongside industry experience from within the Group. This enables the team to provide general risk and business specific assurance. The internal audit team also oversees regional control compliance and undertakes commercial and cost auditing using specialist skilled resource. It continues to maintain a budget for co-sourced expertise to be brought in to provide more specialised reviews, such as IT, and to take advantage of focused data analytics.

During 2024, internal audits were undertaken in accordance with the Committee's agreed plan for the year. Regular updates were provided to the Committee on the status of ongoing audits and action closure. The Committee monitored progress against the plan, discussed the results of all audits undertaken and monitored relevant actions to address recommendations. The internal audit team also supported the internal investigations that were undertaken in relation to the cost forecasting issues in the South Division.

The Board and ELT also commenced activity to address the revisions to the Code, which were set out at the beginning of 2024. The main change, in effect for periods beginning on or after 1 January 2026, concerns strengthening risk management and internal control requirements defined within the updated Provision 29. Principle O now references the need for boards to establish and maintain the risk management and control framework. The Board are fully supportive of this change and are monitoring compliance to the new provisions set out in the revised code through the Audit Committee. A roadmap for full compliance has been approved by the Board, including improvements which are underway to increase the level of formality and Board involvement. These include:

- A significantly enhanced fraud risk assessment with a new supporting process for the identification, review and reporting of both known and potential fraud risks.
- A formal definition of all operational, financial, IT and People related controls to achieve a greater level of standardisation and definition which is supportive of the Group's strategy. New members of the ELT will sponsor each discipline and we have already completed a full refresh of all our life of site operational standards – from procuring land to closing down our completed sites.
- Continued investment in single systems across our Group that support automation of control, with alignment to our quarterly declaration for each region to ensure system usage and standardisation.


- A dedicated auditor within the internal audit team focusing on regional controls and self-assessment follow up and testing.
- Standardised Board control reporting and sign-off processes.

The Committee also considered and approved both the headcount and organisational design of the internal audit team to ensure appropriate scale and expertise. They recommended that, whilst the internal audit function is operating effectively, a greater proportion of the audit plan should be dedicated towards more granular testing of controls, in particular the CVR process following the cost forecasting issues that arose in the South Division during 2024.

The Committee approved the 2025 internal audit plan that provides a balance of thematic reviews across the whole Group, alongside specific audits of regional businesses and individual projects with a focus on the commercial aspect due to faster build and quicker turn of capital. Specific areas of focus for the internal audit team have been agreed as follows:

- Commercial controls compliance
- Partner compliance and customer related processes
- Special Projects
- Performance management
- Modern slavery

ENTERPRISE RISK MANAGEMENT

 The framework and processes the Group operates to manage risk are set out on pages 68 and 69.

During the year, the Committee monitored and reviewed the Group's risk management activities and processes through reports at each Committee meeting. The Committee reviewed the work of the Risk Oversight Committee's bottom-up and top-down process utilised to identify risks, the movement of principal risks, identification of emerging risks and the risk appetite. Following the strategic change, the Committee was updated on how the approach of the Risk Oversight Committee was evolving to reflect the key challenges impacting the Group from external factors, integration and economic factors.

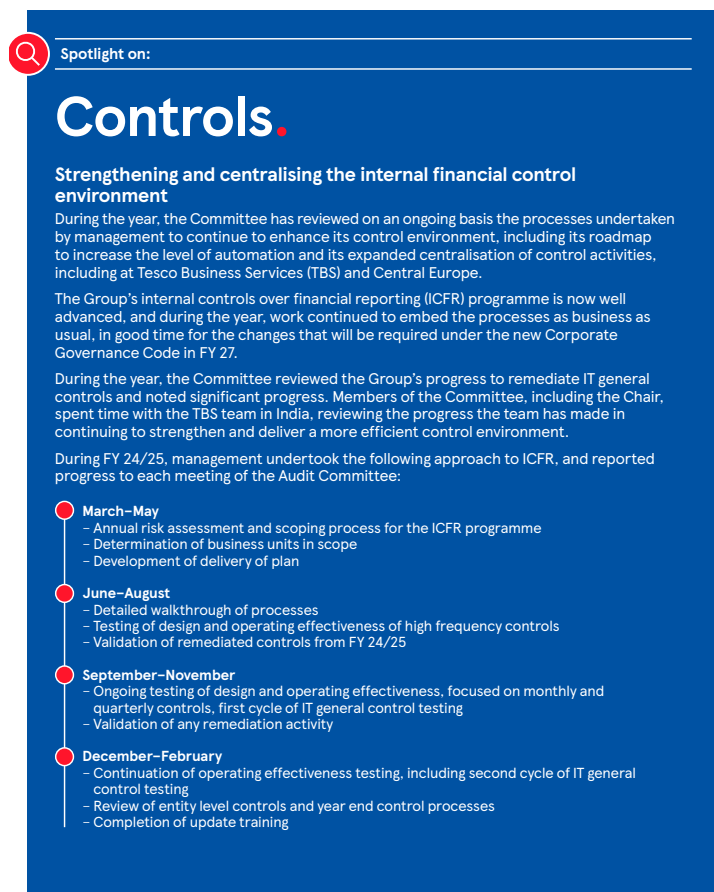
WHISTLEBLOWING

Throughout 2024, the Committee has reviewed the operation of the independent third party managed whistleblower hotline to enable employees and third parties to report matters of concern. The Committee has continued to receive reports on ongoing and concluded investigations. The Committee also considered the actions taken by management as a result of the investigations.

Source: <https://www.vistrygroup.co.uk/sites/vistrygroup/files/2025-04/ara-2024-25-all-spreads-v1.pdf>

Figure 14

Tesco FY25 ARA, p. 84



Internal controls

Through its ICFR programme, management is responsible for maintaining an effective internal financial controls framework, that identifies risks, maps these to controls and gives assurance over the effective operation of its control activities. Management undertakes this through a three lines of defence model, including financial controls testing by a team independent of the relevant control operators and use of the Group's internal audit function as a third line of defence. Such testing includes validation of IT general automated controls as well as manual business process control activities, and entity level controls.

Management is also responsible for identifying and managing risks, and for maintaining the Group's system of internal controls, which is designed to manage and mitigate relevant risks. During the year, on behalf of the Board, the Committee conducted a review of the effectiveness of management's internal controls processes. The Committee did this principally through updates provided to it by management, Group Controls and Compliance, Group Audit, and the external auditor.

During the year, the Committee reviewed the effectiveness of the ICFR framework, including considering the output of the work undertaken by the Group Control and Compliance team, the Group internal audit team and the external auditor. In addition, the Committee has reviewed the work performed by management to embed

ICFR as a business-as-usual activity ahead of the requirements of the new Corporate Governance Code in FY 27, including the process by which the Board will be required to make its declaration under Provision 29 of the Code. As part of this, the Committee reviewed the progress made at TBS to further improve its level of control effectiveness.

The Committee also received regular updates about the progress made by management to remediate and improve IT general controls and IT automated controls and challenged the external auditor to continue seeking to increase the level of reliance on such controls during the audit. As a result, the external auditor has been able to increase its level of reliance on IT general controls over our main financial reporting system as well as certain other key business process areas.

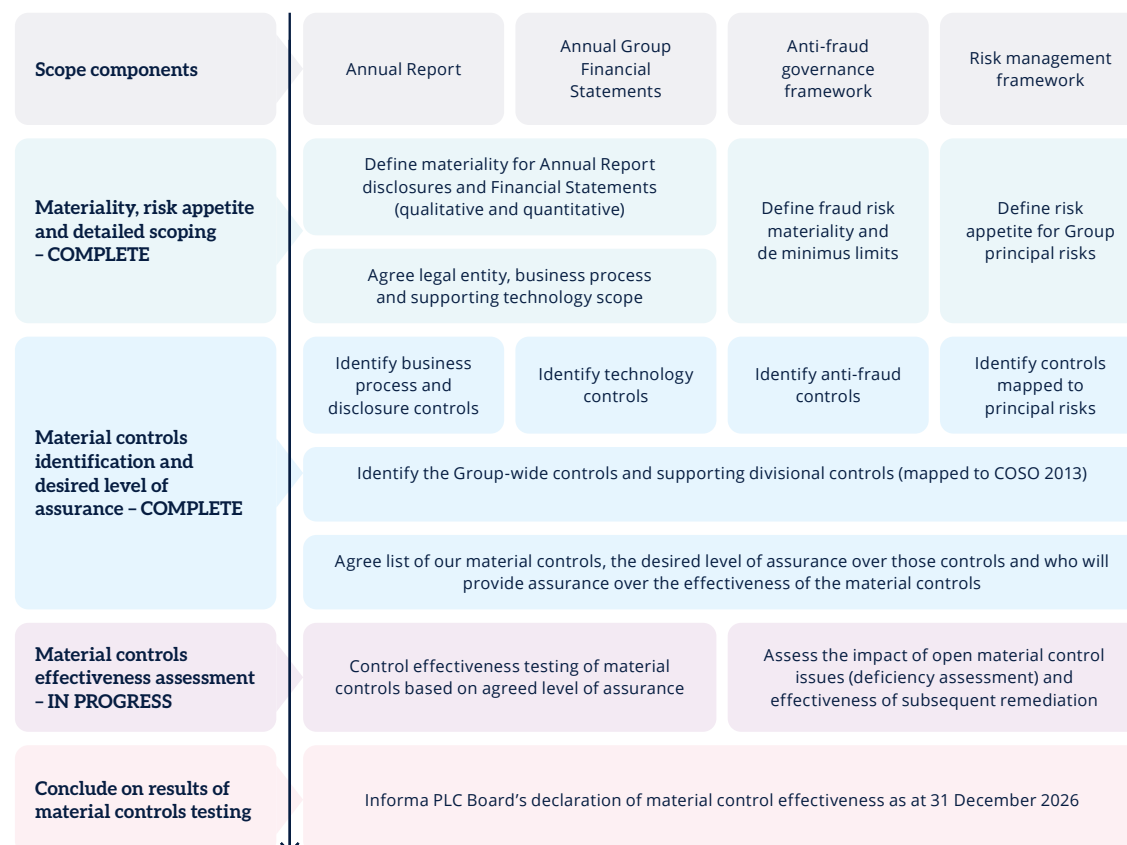


Work continued during the year to embed the ICFR programme as a business-as-usual activity, in good time for the changes that will be required under the new Corporate Governance Code in FY 27.

Figure 15

Informa 2024 ARA, p. 111-112

Process to material controls declaration



Enhancing technology governance

The Committee undertook a deep dive into technology failure risk, noting that a prolonged loss of critical systems could inhibit the company's ability to deliver products and services. We noted that strong progress was being made to mitigate this risk, by fully mobilising the Fortify programme to deliver a new framework and platform for enhanced security, observability and cost control.

We also reviewed the deep-dive exercise undertaken to identify our key applications and received an update on the project to ensure that ownership of each application was appropriately assigned.

Changes to the Code and failure to prevent fraud

In the 2023 Annual Report, we set out the actions taken in response to UK Government reforms to restore trust in audit and corporate governance. While a substantive element of those reforms was withdrawn, during 2024, Informa continued to strengthen its Group-wide and divisional controls – in preparation not only for the requirement in the revised Code for an annual declaration of control effectiveness for financial years beginning on or after 1 January 2026, but also in response to the new corporate criminal offence of failure to prevent fraud (FTPF), which will come into force on 1 September 2025.

Code Provision 29

Early in 2024, management presented a current-state assessment of Informa's control environment in preparation for the declaration of the effectiveness of material controls that will be required for the year ending 31 December 2026. The assessment included details of how and when any control weaknesses or gaps would be remediated.

We reviewed progress against the objectives set for 2024 at each meeting, noting how management's thinking had evolved, and are satisfied that the project continues on track – see diagram below.

As the Informa TechTarget combination progressed, we also considered how the Informa Finance team would work with Informa TechTarget to support the Sarbanes-Oxley compliance work for 2025, and their remediation plan to address the material weaknesses.

Failure to prevent fraud

In November 2024, the UK Government published regulations bringing a new FTPF criminal offence into force and also issued guidance on reasonable fraud prevention procedures.

Earlier in the year, we had reviewed and discussed the recommendations of a KPMG advisory report on Informa's anti-fraud governance framework future development. We noted that, after receiving the advisory report, a plan had been developed to prioritise those KPMG recommendations that were particularly relevant to the FTPF legislation. However, implementation was paused until November, when the guidance was published.

Management advised in December that it would now review and refine KPMG's recommendations to reflect the guidance. We will be scrutinising progress on this during 2025, making sure the implementation timeline is aligned with the offence enforcement date.

Source: <https://www.informa.com/globalassets/documents/investor-relations/2025/2024-informa-annual-report.pdf>

Figure 16

IAG 2024 ARA, p. 122-123, 125

Area of Committee focus	Activities
Enterprise risk management (ERM)	<ul style="list-style-type: none"> • Reviewing the principal and emerging risks facing the Group, including gaining assurance as to the effectiveness of the internal control system, mitigations and risk management process; • Reviewing the principal risks and the combination of risks that possess the potential to significantly impact the Group's strategic objectives, in order to simplify and further refine the Group's risk disclosures; • Reviewing the process whereby the Board reviewed and determined risk appetite; • Reviewing the performance of the Group against its existing risk appetite and confirming management's assessment that the Group has applied appropriate mitigations or other effective controls to ensure that the Group has operated within (or agreed) risk appetite throughout the period; • Reviewing annual compliance with the ERM risk policy; • Reviewing the Group's fraud risk assessment and design of the internal control framework to prevent and detect fraud, including consideration of the key controls and assurance activities provided across the Group in relation to financial and non-financial fraud risk; • Overseeing treasury risk management, including reviewing the Group's fuel and foreign exchange hedging policies, positions and financial counterparty exposure, compliance with the Group's treasury and financial risk management policies and consideration of the implications of the approved fuel hedging profile, given the recovery in demand and significant volatility in fuel prices, and ensuring its continued appropriateness in managing these risks; and • Overseeing tax risk management, in an environment of increased challenge, investigation and audit by tax authorities across the globe, and considering the tax strategy before recommending it to the Board for approval and publishing it on the IAG website.
Non-financial information	<ul style="list-style-type: none"> • Reviewing management's preparations to comply with the Corporate Sustainability Reporting Directive (CSRD) (directive 2022/2464/EU) as well as the integrity of information provided in the Group's Consolidated Sustainability statement in compliance with Law 11/2018, including information on environmental, social, employee and human rights-related matters. In addition, the Committee received the external auditor's limited assurance report and conclusions on the Sustainability statement; • Reviewing the integrity of the reporting and data in respect of the Group's longer-term sustainability and climate-related risks and opportunities, including the Group's alignment with the provisions of the TCFD process, and the appropriate reflection of the implications of climate change in the Group's strategy, financial statements and financial and cash flow forecasts; and • Understanding the phased programme towards readiness for reasonable assurance for non-financial information in respect of key and required sustainability and people/workforce measures and monitoring the significant progress achieved, leveraging the Group's established methodology for implementing internal controls frameworks and defining the controls, accountability and governance essential to achieve effective reasonable assurance.
Matter	Action taken by the Committee and outcome/future actions
Fraud procedures	<p>The Committee examined management's report on the Group's fraud prevention framework, which included the annual fraud risk assessment, the key controls and the lines of defence established to prevent and detect fraud. The Committee observed strong alignment between the risk assessment and the assurance map, including lines of defence, and was satisfied that the approved internal audit plan addressed the key financial reporting anti-fraud controls as well as audits targeted at specific fraud risks across the Group during this period.</p> <p>Management updated the Committee following the November 2024 release of the implementation guidance for the UK Economic Crime and Corporate Transparency Act 2023. The Committee will oversee management's response to the guidance, particularly regarding reasonable procedures to prevent fraud and any necessary enhancements to the Group's fraud prevention framework.</p> <p>On behalf of the Board, the Committee will continue to monitor fraud and internal controls, including consideration of feedback from the external auditor, the outcomes of the annual ICFR audits and the results of a series of focused anti-fraud control internal audits.</p>

Source: <https://www.iairgroup.com/media/4qxgaavc/iag-annual-report-and-accounts-2024.pdf>

Figure 17

GSK 2024 ARA, p. 44, 56, 132, 141

AI Governance: Our Responsible AI framework helps us maintain clear guardrails as we scale adoption of AI across GSK to drive innovation, growth and productivity and, in doing so, to accelerate our purpose.

In my report last year, I described the establishment by the Board of the AI Governance Council (Council), its purpose and activities that helped to define, establish and oversee these guardrails. The Council is aligned to the ROCC and Committee's reporting arrangements, as well as our other governance forums, as appropriate. A year after the Council's creation, the Committee was keen to examine the:

- structure and evolving operational effectiveness of the Council
- functioning of the responsible AI governance architecture, including the complementary roles, duties, ownership and composition of each of these AI forums
- overall increase in maturity of our AI risk management arrangements

The Committee was pleased with the significant initiatives that the Council had pursued and rolled out across the Group to further enhance GSK's AI environment. These included:

- approving an AI Policy that embeds new AI principles and establishes guidelines for use of AI within the company. The Policy applies to all AI developed, procured, or used by our people at GSK. Responsible AI training modules continue to be rolled out
- developing, adopting and publishing an AI Standard Operating Procedure (AI SOP), defining steps required for all development and/or procurement of AI systems across GSK
- monitoring an inventory of all AI models developed across GSK. This is being actively monitored through the Council, as the number of AI applications in use expands at pace across the enterprise

The Committee received a briefing from the Head of Audit & Assurance (A&A) on the results of an initial audit, that primarily focused on evaluating how the AI Governance framework is embedding across GSK. This has also helped strengthen oversight capabilities by increasing the experience of the A&A team in conducting audits and oversight of new technologies.

In 2025, the Committee is looking forward to monitoring how the Council progresses its key focus areas. These include:

- supporting business units in further improving and refocusing their AI systems to align to the AI SOP
- continuing to embed and grow the Responsible AI SOP adoption throughout the organisation
- continuing to oversee and monitor AI systems, including developing technical and operational best practices
- refining and maturing the Council's governance approach for scaled adoption of AI across GSK

During the formative stage of AI development and adoption, the Committee is keen to ensure an appropriate balance is maintained between identifying, mitigating and monitoring key AI risk areas across the enterprise and with our third parties, while harnessing the opportunities and capabilities of this technology.

Data technology and accelerating GSK's ambition

The Board reviewed and endorsed plans, including progress made on our AI adoption strategy

The Board reviewed and provided feedback on the technology priority objectives and management's approach to integrating technology into the core of GSK. In particular, AI represented a transformative opportunity for patient and shareholder impact, with a focus on achieving significant breakthroughs in scientific innovation, target identification and accelerating the progress of our pipeline

While the opportunities presented by AI are clear and would be progressed at pace, this would need to be balanced against:

- People and change: enlisting everyone at GSK in this effort and increasing digital fluency across the company
- Data & Trust: meeting and maintaining the highest standards with regard to trust and integrity in how we use and manage data
- External healthcare ecosystem: assessing the ecosystem of healthcare providers, payers and regulators for digital opportunities and risks to manage

The Audit & Risk Committee also undertook a review of the evolution and operational effectiveness of our AI Governance arrangements

Stakeholders: Patients, employees, investors, governments and regulators, healthcare providers, payers
Other s172 duties: Our long-term results, workforce and business relationships

Using data and AI responsibly

We take our responsibility for data ethics and privacy seriously and we exercise high standards of integrity in dealing with the personal information of our employees, patients, clinical research participants, healthcare providers and other stakeholders.

Our Digital and Privacy Governance Board oversees our overall data ethics and privacy operating model, supported by digital and privacy legal experts and compliance professionals. The board monitors fast-evolving legislation, regulations, guidance and requirements being published by global regulators.

Cyber security threats have become more sophisticated and are increasing with our expanding digital footprint. We deploy cyber security controls, monitor and mitigate new and emerging cyber threats to protect GSK from cyber security risks.

In 2024, we continued to embed our cross-functional AI Governance Council (AIGC) to oversee our AI strategy and to ensure responsible adoption of AI/ML. We also introduced a new responsible AI Standard Operating Procedure, which defines the requirements for all development and/or procurement of AI systems across GSK, and established a framework for business functions to integrate AI risk review and management within existing risk management compliance boards. Our public policy position on responsible AI sets out our views, commitments and asks of policymakers.

Harnessing technology

Technology is transforming how we manufacture medicines and vaccines, enabling us to increase the speed, quality and scale of product supply.

Technology helps us optimise efficiency and effectiveness across our operations. We're reducing cycle time and cost in the Chemistry, Manufacturing and Controls (CMC) development process, the manufacturing and quality processes as well as the end-to-end supply chain and distribution processes.

We're using data to help us monitor production in real time, spot ways to increase yields and predict when equipment needs maintenance.

We're using smart manufacturing technologies for greater efficiency, productivity, sustainability and cost savings. Smart manufacturing is not about replacing people with technology, it's about enabling us to work smarter and more efficiently. We can augment our human creativity, expertise and problem solving with data and AI, increasing our impact and delivering better and faster for patients.

For example, we have introduced an AI tool to quickly determine the best transportation route to deliver our medicines and vaccines to patients. The tool does this by analysing vast amounts of data, including stock availability, cost, carbon emissions and batch details such as readiness to ship at a given time. As a result, we can save costs, reduce carbon emissions and make sure stock reaches its destination on time for patients.

Figure 18

Pets at Home FY25 ARA, p. 20, 29, 39, 44

Material Controls

The ARC receives bi-annual updates on internal controls. During the year, we have made progress in planning for compliance with the requirements of the UK Corporate Governance Code 2024. Key activities include:

- Defining material controls
- Enhancing our Risk and Control framework with particular focus on data governance, AI, pet welfare and improvements in the operation of some key IT operational controls
- Agreeing our assurance approach

These will remain key areas of focus as we continue to embed control improvements ahead of our March 2027 compliance date.

Risk management systems and internal controls

Risk management and the system of internal control are the responsibility of the Board. It ensures that there is a process in place to identify, assess and manage significant risks that may affect achievement of the Group's objectives and that the level and profile of such risks is acceptable (based on the Board's risk appetite). The processes have been in place for the year under review and up to the date of approval of the Annual Report and Accounts.

The Committee provides oversight and challenge to the assessment of principal risks as set out on page 20. The Committee has continued to monitor and challenge the control environment of the Group including its general risk management, risk register and internal controls processes, as well as emerging and evolving risks considering the presence of key risk factors. This has included assessment of the likelihood and impact of principal risks materialising, and the management and mitigation to reduce the likelihood of their incidence or their impact. The Committee explores specific principal and corporate risks of the Group in detail, inviting the management team to discuss the risks, mitigations and further proposed actions. In 2025 the key topics covered in deep dives were cyber security, data privacy, business continuity planning, the pace of replacing ageing technology assets as well as health and safety.

During the year the Executive team have refreshed the risk management process ensuring new divisional leaders have clearly framed the risks in the context of the current economic backdrop, have articulated their risk appetite more precisely and set up regular monitoring of mitigations and the acceptability of residual risks carried by the Group. Skills in the central risk team have also been strengthened under the leadership of an experienced manager and the recruitment of a professionally qualified risk professional. Taken together this will better support the Committee's work on effective risk management.

The Group's principal risks and uncertainties are set out on pages 21 to 29. The three lines of defence governance model is set out on page 19 along with the Board's risk management process.

The Committee has monitored the progress of the internal controls enhancement project which has progressed well, being focused on improving the internal control environment whilst adapting to changes to the UK Corporate Governance Code.

The material controls have been defined and the control gaps and areas which require further remediation are being worked through. The principal risks have been considered and cascaded down to the material controls.

Most core business processes and related risks and controls have been documented. Key processes have been assigned to business owners and recommended actions to improve control weaknesses and the maturity of the control environment are being implemented. These relate to the retention of evidence, segregation of duties and the formality and consistency of control operation. We continue to have a strong focus on IT controls where the initial documentation is substantially complete, and our work continues to be focused on control improvements. In line with the FRC recommendations, the focus has also broadened to include non-financial controls, including business processes and controls across cyber security, pet welfare standards as well as data as an asset and data integrity. We have agreed our audit and assurance policy to guide the Committee's work in assessing effectiveness of material internal controls and implemented enhanced first and second lines of defence.

Information security and business critical systems, including cyber security risk, continues to be one of the Group's Principal Risks and an area we remain vigilant over given the increasingly complex nature of cyber attacks. We continue to review and improve our cyber protection approach, test and refine our incident response processes, including incident rehearsals strengthening the underlying framework. We are also reviewing our business continuity and disaster recovery capabilities in order to identify improvements in these areas. The Committee has reviewed the effectiveness of data protection policies, training plans and compliance.

AI is being used increasingly across the business to enhance efficiency, support innovation and improve the consumer experience. It brings complex risks and requires controls and guardrails over development, deployment and performance. The Committee has overseen the development of the AI governance framework, which is a material control framework, to ensure the framework is appropriate and the Acceptable Use Policy has been appropriately rolled out across the Group.

The Committee has reviewed health and safety performance reports twice in the year, including strategies and action plans developed by management. The Committee has also reviewed the effectiveness of the Group's whistleblowing procedures, and incident reports are reviewed regularly. Compliance with codes of conduct and culture and other key policies such as anti-bribery and corruption, anti-money laundering, and compliance with the Companies Act are conducted on an ongoing basis.

The Committee has reviewed the fraud effectiveness framework and the profit protection framework, including an update on the business assessment of fraud risks.

The Committee has continued to monitor the progress and delivery of major projects throughout the year including the digital platform and capability (Project Polestar), the pilot phase of the new practice management system within the Vet Group (Project Darwin) and the completion of the transition of our multichannel operations to our new distribution centre in Stafford (Project Spice), building on the lessons learned analysis carried out by the Board in relation to the transition of our store operations to Stafford. During the year the Committee appointed an independent and deeply experienced leader to provide assurance over the delivery of Project Darwin and to embed more rigorous disciplines over transformation programmes following the lessons learnt analysis.

The Committee has also performed risk reviews with management on several risk areas in the year including a review of treasury policy, ensuring it remains appropriate for the Company, and has overseen the adequacy of insurance coverage over material risks for the Group, and the maintenance of appropriate standards of pet welfare.

The Board, through the Audit and Risk Committee, are satisfied that the internal control framework is effective but acknowledges that the Internal Controls project is progressing to enhance the risk management process and internal financial controls, which both the Board and Committee will continue to monitor in FY26.

Legal and compliance

Owner: Chief Financial Officer

Risk Type: Financial

Links to strategy 1 2 3 4 5 6 7 8 9

Risk profile L M H

Risk appetite L M H

Change on previous year: <>

Description

Many of the Group’s activities are regulated by national and international legislation, applicable industry regulations and standards including, but not limited to, consumer and competition laws and regulations, trading, advertising, packaging, product quality, health and safety legislation and guidance, pet shop licensing, National Minimum Wage and National Living Wage, Equality Act, modern slavery, anti-bribery and corruption, data protection, environmental regulations, the Corporate Governance Code, the RCVS Code of Professional Conduct for Veterinary Surgeons, and the off-payroll regulations (IR35). There have also been significant global developments in artificial intelligence technologies and a regulator-led approach to AI regulation, together with the upcoming implementation of the EU AI Act which has extra-territorial effect. Failure to comply with the obligations set out in this paragraph and other applicable legislation or recommendations of any regulatory investigations may lead to financial penalties and reputational damage and other consequences for the business and its Directors.

Key responses

- We actively monitor regulatory developments in the UK and Europe (as applicable) and our existing obligations where we have internal policies and standards to ensure compliance where appropriate. Training is provided for colleagues.
- We operate a confidential whistleblowing hotline for colleagues, Practice Owners, suppliers, and people working within our supply chain to raise concerns regarding any potential breach of legal or regulatory obligations in confidence.
- Our suppliers commit to comply with all relevant business regulations for the territories in which they operate and to meet international labour standards which are laid out in our Supplier Code of Conduct. We reinforce this by placing contractual obligations on our suppliers and support where necessary.
- The Group’s Data Protection Officer and Executive sponsored Steering Committee monitors Group compliance with legal requirements relating to personal data, ensuring relevant policies are up to date and works with our Information Security Steering Committee which monitors data security.
- We understand the value of ongoing training and communication to raise awareness of the personal data handled by the business, how to keep it safe and how to help prevent personal data incidents. We carry out regular induction, awareness, and refresher training for all our colleagues in Retail, Vets, and the Support Office.

Outlook and further actions planned

- We continue to monitor legal and regulatory developments across the UK and Europe and will plan accordingly.

Emerging risks

- New and amended regulations.
- Significant strengthening of UK consumer laws and regulations including those on the use of digital information, and increasingly stringent environmental regulation.
- Sector review and market investigation by the CMA into veterinary services for household pets in the UK.
- Increasing AI use and regulation.

Risk appetite

The Group is committed to acting ethically, lawfully, and always in the best interests of our stakeholders and therefore has an extremely low appetite for compliance breaches, either regulatory or of our principal internal policies, including for example, our Health and Safety policy and our Code of Business Ethics and Conduct. Anyone who acts on our behalf is expected to act in line with our policies, values, and behaviours and to take the necessary steps to comply with applicable laws and regulations.

On track for Provision 29 compliance | 77

Board Skills Matrix

	Director						
	Ian Burke	Zarin Patel	Roger Burnley	Natalie-Jane Macdonald	Garret Turley	Lyssa McGowan	Mike Iddon
Pet Owner	✓	✗	✓	✓	✗	✓	✓
Expertise							
Accounting, Finance and Audit	✓	✓	✓	✗	✗	✗	✓
Risk Management	✓	✓	✓	✓	✗	✗	✓
Regulatory	✓	✓	✓	✓	✓	✗	✓
Governance	✓	✓	✓	✓	✓	✓	✓
Corporate Transactions (M&A)	✓	✓	✓	✓	✓	✓	✓
International (running a non UK Business)	✓	✗	✗	✗	✗	✗	✓
General Management (CEO)	✓	✓	✓	✓	✓	✓	✓
People and Culture	✓	✓	✓	✓	✓	✓	✓
General Retailing Experience	✓	✓	✓	✓	✗	✓	✓
Customer Service and Communications Experience	✗	✓	✓	✓	✗	✓	✓
Online Retailing Experience	✓	✓	✓	✓	✗	✓	✓
Marketing/Branding	✓	✓	✓	✓	✗	✓	✓
General Services	✓	✗	✓	✓	✓	✓	✗
Veterinary	✗	✗	✗	✗	✓	✗	✗
Healthcare	✗	✗	✗	✓	✓	✗	✗
Charity/Social Purpose	✓	✓	✓	✓	✓	✗	✓
Data	✗	✓	✓	✓	✗	✓	✗
Artificial Intelligence	✓	✓	✗	✗	✗	✗	✗
IT and Technology	✗	✓	✓	✗	✗	✓	✗
Omnichannel	✓	✓	✓	✓	✗	✓	✓
Strategic Leadership	✓	✓	✓	✓	✓	✓	✓
Vision and Mission	✓	✓	✓	✓	✓	✓	✓
Sustainability and Climate Change	✓	✓	✓	✓	✓	✗	✗
Transformation Leadership	✓	✓	✓	✓	✗	✓	✓
Chair of PLC Board	✓	✗	✗	✗	✗	✗	✗
Chair of PLC Board Committee	✓	✓	✓	✗	✓	✗	✓

Source: <https://www.petsathomeplc.com/media/pmzbckb2/47627-pets-ar25-web-160625.pdf>

Figure 19

Tesco FY25 ARA, p. 64



Source: https://www.tescopl.com/media/ky0bfwpo/tesco_ar25_interactive.pdf

Figure 20

Legal & General 2024 ARA, p. 47

Our risk management framework

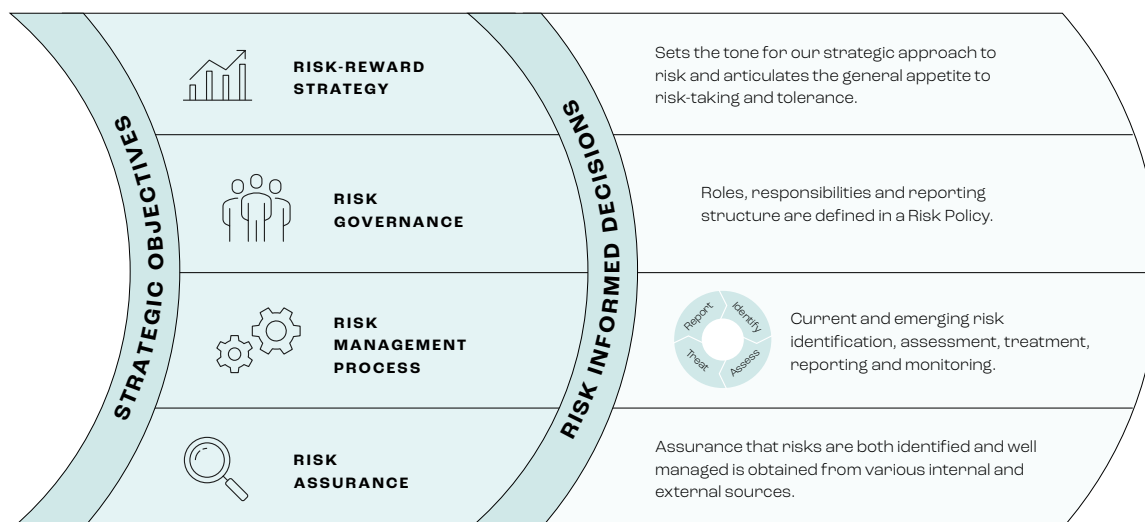
Risk appetite	The documenting of the Group's overall attitude to risk and the ranges and limits of acceptable risk taking.
Risk taking authorities	The formal cascade of our risk appetite to managers, empowering them to make decisions within clearly defined parameters.
Risk policies	Defines required approaches to managing specific risks so that residual exposures are within appetite.
Risk identification and assessment	Tools and resources to help managers identify and evaluate the risks to which we may be exposed.
Risk management information	How we report and review ongoing and emerging risks and assess actual risk positions relative to the risk targets and limits that we set.
Risk oversight	Oversight of risk management by L&G's risk teams.
Risk committees	Group-level Committees oversee the management of risks and challenges how the risk framework is working. The role of the Group Risk Committee is set out on page 61.
Culture and reward	Performance measures that focus on the delivery of effective risk management, business and customer and client strategy, and culture.

Source: <https://group.legalandgeneral.com/media/2rcpejt1/l-g-annual-report-and-accounts-2024.pdf>

Figure 21

PPHE 2024 ARA, p. 91-92

Our risk management framework



Our risk-reward strategy

Our risk-reward strategy, which articulates our risk appetite across various business activities, is aligned to our strategic objectives. The Board has reassessed the strategy and adjusted the risk appetite for Technology change and development to Active, indicating a more proactive stance on adopting new technologies.

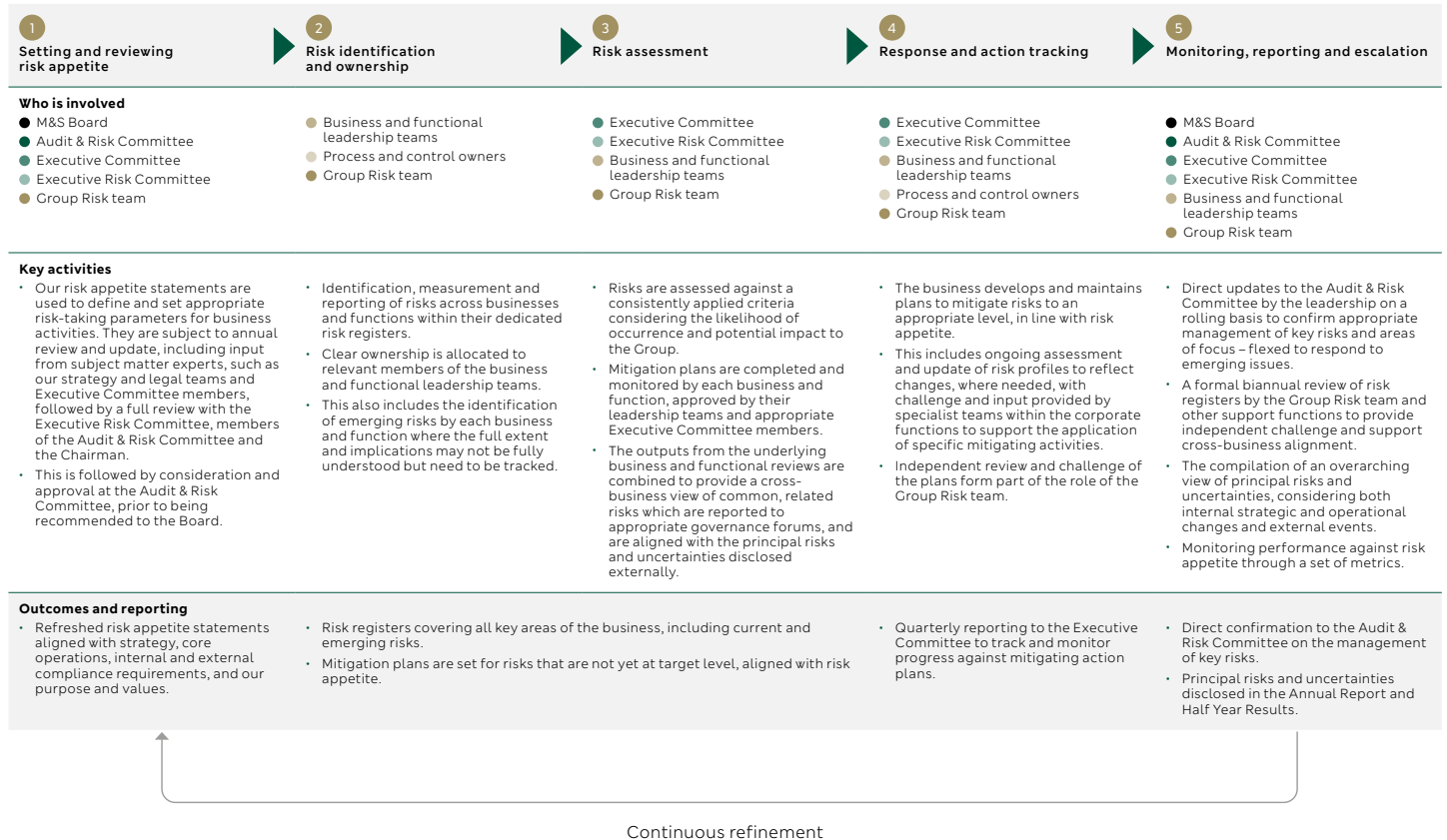
Risk appetite levels	Definition	Business activities	Strategic pillars and enablers
Active	We will actively seek to take calculated risks in this area in pursuit of our strategic objectives, as long as the associated benefits significantly outweigh the risk impact, and the risk remains within our tolerances. We will apply appropriate safeguards when pursuing these opportunities.	<ul style="list-style-type: none"> Acquisitions and development opportunities Technological change/development 	Diversification of property portfolio Entrepreneurial, people-oriented and creator culture to underpin growth agenda
Neutral	We will take on a limited increased exposure to risk in pursuit of our strategic objectives if the associated benefits outweigh the risk impact and the risk remains within our tolerances. We will apply appropriate safeguards when pursuing these opportunities.	<ul style="list-style-type: none"> Development projects (construction) Working with third parties Funding Commercial and promotional activity 	Non-dilutive capital approach Destination led restaurant and bar experience with ambitious growth plans Entrepreneurial, people-oriented and creator culture to underpin growth agenda
Averse	We will act to protect the business from increased risk exposure in these areas.	<ul style="list-style-type: none"> Environmental impact Responsible and ethical sourcing Human rights Operational continuity Health and safety Data privacy Compliance Financial and tax reporting Financial control 	Meaningful ESG impact for the benefit of all stakeholders Guest satisfaction – memorable and superior guest experiences

Source: https://ar24.pphe.com/wp-content/uploads/2025/02/PPHE_ARFull_2024.pdf

Figure 22

M&S FY25 ARA, p. 53

Our risk management process



Source: https://corporate.marksandspencer.com/sites/marksandspencer/files/2025-05/Marks-and-Spencer-Group-plc-Annual-Report-and-Financial-Statements-2025-INTERACTIVE_FINAL.pdf

Figure 23

Fresnillo 2024 ARA, p. 118-120

Risk management process

Set strategy, objectives and risk appetite	1. Risk analysis Identify, prioritisation and evaluate risks to our strategy and objectives	2. Controls and risk responses Implement controls and actions to manage risks within risk appetite	3. Audit & assurance Check and verify that controls and actions are effective in managing the risks	4. Communication & monitoring Communicate principal and emerging risk and escalate as appropriate	5. Improvement & embed Build risk capability and culture so active management is embedded in how we run our business	6. Resilience Development of the Company's culture and capacity to adapt, resist, absorb and recover from the impact of a risk
First line	<ul style="list-style-type: none"> Risk assessment and identification of new risks in the business units. 	<ul style="list-style-type: none"> Continuous improvement of processes and controls. Implementation of corrective and preventive actions based on the results of leadership team monitoring. 	<ul style="list-style-type: none"> Control self-certifications. 	<ul style="list-style-type: none"> Preparation of risk dashboards and risk matrices presenting the status of individual risks in the business units. 	<ul style="list-style-type: none"> Compliance with the highest international industry standards such as TSFs. 	
Second line	<ul style="list-style-type: none"> Review of Key Risk Indicators (KRIs) and mitigation actions. 	<ul style="list-style-type: none"> Implementation of controls and mitigations in response to risk scenarios. 	<ul style="list-style-type: none"> Monitoring compliance with international risk standards. 	<ul style="list-style-type: none"> On-going reviews of risks and threats. Preparation of quarterly, half-yearly and Annual Reports and briefings to the Audit and HSECR Committee. 	<ul style="list-style-type: none"> Promoting the risk culture across the Company through workshops and training. 	<ul style="list-style-type: none"> Creating risk scenarios to anticipate impacts and prepare risk responses.
Third line			<ul style="list-style-type: none"> Execution of the annual internal audit programme. 	<ul style="list-style-type: none"> Advice and recommendations regarding the most exposed or new risks. 		<ul style="list-style-type: none"> Implement appropriate policies and guidelines to build resilience to risks.
Culture & leadership						

3. Audit and assurance

The Board, in pursuing the Company's business objectives, cannot give absolute assurance that the implementation of a risk management process will overcome, eliminate, or mitigate all material risks. However, by developing and implementing an annual and ongoing risk management process to identify, report and manage significant risks, the Board intends to provide reasonable assurance against material misstatement or loss.

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:

The internal audit team consists of highly experienced professionals from various specialties, who frequently review operational, financial, exploration and project processes in the field, using international standard tests and methodologies.

First line	<ul style="list-style-type: none"> Annual self-assessments of controls and the bi-annual compliance assurance statements.
Second line	<ul style="list-style-type: none"> As part of our ERM approach, we the Risk Team conduct specialised reviews to assess risks and controls to ensure compliance, focused on validating and testing key controls to augment the first line attestations. The risk team annually reviews key controls for our principal risks, significant local risks and response plans to identify and respond to any significant changes in the control environment. Whilst many controls are tailored to business unit requirements, there are consistent themes across our control environment, such as clear oversight and reporting by business unit management teams, governance processes for operations, maintenance and tenders, attention to health and safety, the wellbeing of our people and the priority of maintaining integrity and a strong ethical culture.
Third line	<ul style="list-style-type: none"> We are supported by external partners in certain specialised areas, we are also subject to significant assurance activities and third-line audits conducted through our Internal Audit team, external third parties, certification standards and customer requirements in our various business lines. The work plan of the internal audit area considers all the company's operational and financial processes, permanently following up on the recommendations made in each audit, with a particular focus on the most exposed risks or risks that have an impact on regulatory non-compliance or business disruption. 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 Fresnillo plc operations. Examples include: <ul style="list-style-type: none"> business continuity risk inspections of all business units by Hawcroft Consulting in 2024. ISO 45001 and ISO 14001 audits of Fresnillo and Saucito mines by BSI Group auditors. certification that the Herradura mine leaching operations comply with the Cyanide Code issued by the International Cyanide Code Institute.

Source: <https://www.fresnilloplc.com/media/zqcbodxt/46566-fresnillo-ar24-web.pdf>

Figure 24

3i Infrastructure FY25 ARA, p. 63

Risk categorisation

The Committee uses the following categorisation to describe risks that are identified during the risk review process.



Source: <https://www.3i-infrastructure.com/media/p3fajhc2/3i-in-annual-report-2025.pdf>

Figure 25

discoverIE FY25 ARA, p. 70

Two processes are conducted in parallel:	
Step 1 <ul style="list-style-type: none"> ▪ A top-down review of the Group Risk Register to: <ul style="list-style-type: none"> – identify new or emerging risks – assess changes to existing risks – consider the potential impact and likelihood of risks – evaluate existing mitigating actions and controls – consider the residual risks remaining after the applications of the Group's internal control processes (and if appropriate, the implementation of further mitigating actions) <p>The top-down review of the Group Risk Register is conducted by the Group Risk team, Divisional Management, Group Technology Services, and the internal Group Sustainability Team. The bottom-up review is conducted by the management team within each business with support from the Risk team.</p>	<ul style="list-style-type: none"> ▪ A bottom-up review by the management of each business to: <ul style="list-style-type: none"> – identify new or emerging risks – assess changes to existing risks – consider the potential impact of risks – evaluate existing mitigating actions and controls – consider residual risks (and if appropriate the implementation of further mitigating actions)
Step 2 <ul style="list-style-type: none"> ▪ Comparison of the results of the top-down and bottom-up identification processes above. The benefits of conducting both top-down and bottom-up reviews are: <ul style="list-style-type: none"> – increased assurance that all risks have been identified, with input from multiple perspectives – ensuring alignment between local management and Head Office – ensuring that businesses take ownership of the risks most relevant to their individual operating unit – ensuring that controls in place to mitigate risks at the operating unit level are appropriate ▪ An assessment of any differences identified and update of the Group Risk Register as appropriate. The Group Risk team conducts a review of any risks identified through the bottom-up process to determine whether they require escalation to the Group Risk Register. Risks suggested for escalation to the Group Risk Register are reviewed in the first instance by the Group Management Committee. 	
Step 3 <ul style="list-style-type: none"> ▪ Review of the Group Risk Register by the Group Management Committee. This review focuses on: <ul style="list-style-type: none"> – the materiality of each of the risks identified – prioritisation of the allocation of the Group's resources to the most important areas – clarity of ownership for each of the risks identified <p>This review takes into account the Group's risk appetite in respect of the various types of risk identified.</p> <p>The Group Risk Register is then updated as appropriate following the review.</p> <p>This is then summarised in a table of principal risks and uncertainties, the final version of which (for FY2025) is set out on pages 73 to 78.</p>	
Step 4 <ul style="list-style-type: none"> ▪ Review by the Audit and Risk Committee – this includes: <ul style="list-style-type: none"> – consideration of the Group's risk management framework – review of the Group Risk Register – identification of any other areas of potential risk – review of the table of principal risks and uncertainties – challenging actual or potential control weaknesses – review of the effectiveness of the Group's internal controls and risk management systems 	

These processes are conducted twice each financial year:

- an interim review, typically completed shortly ahead of announcement of the Group's interim results, focuses predominantly on changes during the first half of the year
- a comprehensive review of all risks within the Group Risk Register is completed shortly prior to the Group's full-year preliminary results announcement

Source: https://s201.q4cdn.com/793451358/files/doc_financials/2025/ar/Annual-Report-2025.pdf

Figure 26

Severn Trent FY25 ARA, p. 70

We define Emerging Risks as upcoming events which present uncertainty, and those that we are currently monitoring as a potential threat. These Emerging Risks are not yet fully quantifiable, but we monitor developments carefully. The SRF, Executive Committee, Audit and Risk Committee and Board have carried out a robust assessment of the Group's Emerging Risks.

Emerging Risk management ensures potential risks are identified, with plans evaluated to bolster the Group's preparedness should they materialise. Our processes aim to identify new and changing risks at an early stage and analyse them thoroughly to determine the potential exposure for the Group.

We continually identify and monitor Emerging Risks using top-down and bottom-up processes. Our risk network uses techniques such as cross-functional workshops and Political, Economic, Sociological, Technological, Legal and Environment ('PESTLE') analysis.

This process culminates in an Emerging Risk Horizon Scan document which is shared with the SRF, Executive Committee, Audit and Risk Committee and Board on a regular basis.

We closely monitor Emerging Risks that may, with time: become complete ERM risks and incorporated into the existing corporate risk reporting process; be superseded by new Emerging Risks; or cease to be relevant as the internal and external environments in which we operate evolve.

The horizon-scanning exercise utilises insights from internal stakeholders and external publications, including the National Risk Register and Global Risk Report (World Economic Forum). This is critical to reflect the interconnectivity with national and global risk environments.

Details of the Emerging Risks	Relevant Principal Risk	Time Horizon
Geopolitical escalations and macroeconomic changes <ul style="list-style-type: none"> Geopolitical volatility could potentially intensify, including the escalation or resurgence of conflicts. This could result in sanctions and increased protectionist measures, such as US and reciprocal trade tariffs, causing a contraction in the economy and our supply chain could be impacted through shortages, increased commodity prices and resource security pressures. Risk mitigation example: We perform supplier heat-mapping for our contracted supply chain, incorporating financial stability and global economic factors. These provide early warning indicators to manage supply chain risks and facilitate tactical and strategic decision making. 	5, 6 and 8	Short-term and medium-term
	Strategic Objectives	How we are monitoring
	Outcomes	– Horizon scanning
	Nature	– Emerging Risks tracker
	People	– National Risk Register
	Change	– Supplier heat-mapping
Evolving political, regulatory and legislative landscape <ul style="list-style-type: none"> We are subject to ongoing regulation and associated regulatory risks, including the effects of changes in the laws, regulations, policies and voluntary codes of practice. Regulators and Governments have focused on reforming the UK water sector. The Independent Commission into the water industry and its regulators – led by Sir Jon Cunliffe – was launched by the Government in October 2024 to address challenges facing the sector. The Commission is seeking the views of stakeholders to shape the outcomes of the review, with the strategic objective of restoring trust in the water industry. The Water (Special Measures) Act 2025 strengthens the power of the water industry regulator and delivers on the Government's commitment to restore public trust and confidence in water companies. Our horizon scan references the potential impact on culture, people, environment and customer-related activities. Risk mitigation example: We continue to engage constructively with our key stakeholders to ensure we remain informed and are proactively preparing for potential changes. 	2, 3 and 7	Short-term and long-term
	Strategic Objectives	How we are monitoring
	Outcomes	– Horizon scanning
	Nature	– Emerging risks tracker
	People	– Existing ERM risks
	Change	– Stakeholder engagement
Technology and innovation, including AI and cyber security <ul style="list-style-type: none"> Technological advancements present opportunities to develop new and innovative ways of working through the automation of basic activities and increased processing power to support decision making (e.g. maintenance schedules). However, we need to develop AI in an ethical way to address potential concerns and mitigate against an increasingly complex cyber and data security environment. There is an increased risk of misinformation and disinformation as AI content becomes more prevalent and the speed at which it disseminates increases, partially driven by social media and changes to fact-checking procedures. The UK signed the Council of Europe's Framework Convention on AI in September 2024 and in January 2025, the Labour Government launched a detailed AI action plan setting out the steps that the UK aims to take, with the objective of boosting economic efficiency and growth. As AI evolves, this presents both risks and opportunities. Risk mitigation example: We have robust governance in place for AI and an Innovation Strategy to ensure we are embracing opportunities. 	4, 7 and 11	Short-term and medium-term
	Strategic Objectives	How we are monitoring
	Outcomes	– AI Forum
	Nature	– Emerging Risks tracker
	People	– Existing ERM risks
	Change	– Additional risk assessments

Source: https://www.severntrent.com/content/dam/stw-plc/Severn_Trent_AR25.pdf

Figure 27

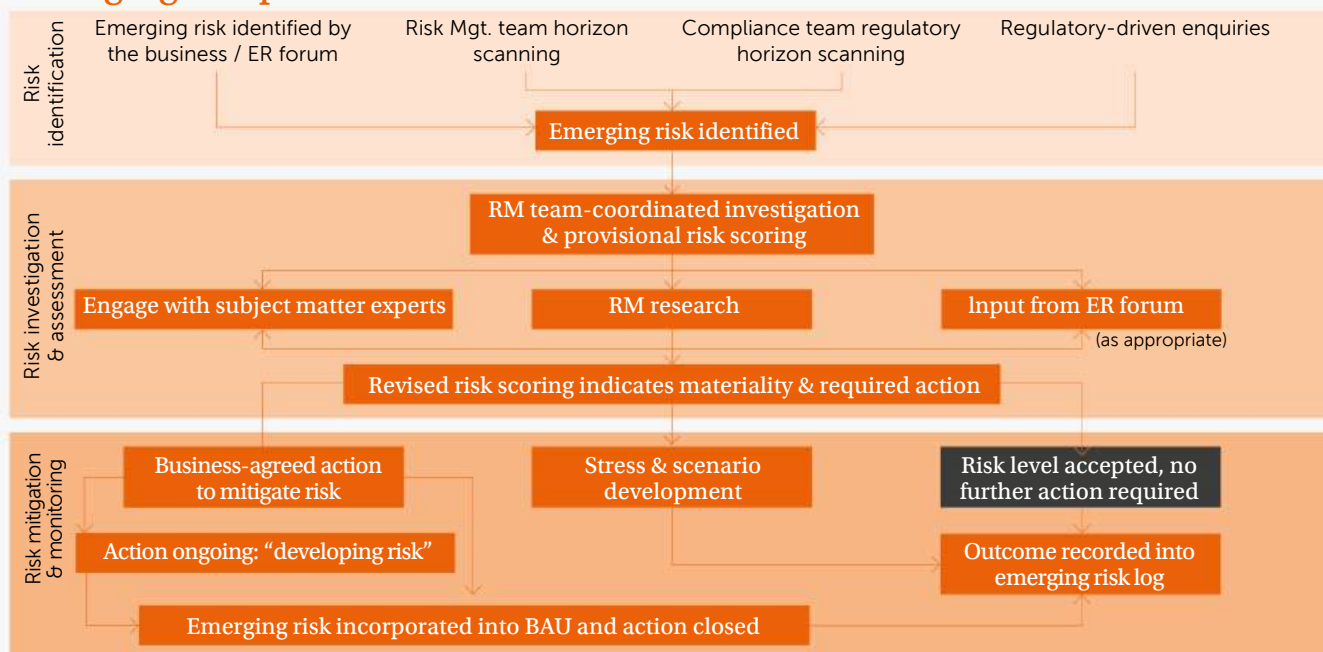
Lancashire 2024 ARA, p. 28-29

Emerging risk

Lancashire defines emerging risk as a change in, or change in understanding of, the internal or external risk environment that could impact the validity of assumptions relating to strategy, decision-making and/or risk management approach. An emerging risk can arise in three ways:

- A genuinely new source of risk that has not existed before;
- A change in the way that an already identified risk can manifest which may not be adequately managed through Lancashire's current risk management procedures; or
- A change in understanding of an already identified risk.

Emerging risk process



The process by which emerging risks are identified, investigated, assessed and reported is illustrated in the diagram on the previous page.

Emerging risks are identified by both the risk management function and the business, and are considered at the emerging risk forum, a Group-wide forum with cross-functional membership. A detailed log of all emerging risks identified is maintained including the anticipated

impact, likelihood, time horizon, velocity, longevity, risk sector, risk type and any actions required.

The top emerging risks for the Group are recorded on our emerging risk radar and discussed with risk owners, executive committees, the Board and entity boards of directors on a periodic basis. The emerging risk radar is therefore subject to an iterative process of review and oversight. During the year, oversight of the



following risks moved to our business-as-usual risk management processes: climate change, operational strain (driven by growth), geopolitical risk, inflation, tax and regulatory change, OECD global minimum tax and Bermuda CIT, and cyber security risks. As a result, emerging risk discussions predominantly focused on artificial intelligence, the many different components of AI and our risk appetite for utilising them.

Figure 28

Morgan Sindall 2024 ARA, p. 57, 62, 104

E. Partner insolvency and/or adverse behavioural change

Some partners may have been trading with stretched finances following the pandemic, the unwind of government measures introduced to support business recovery, and the reverse-charge VAT initiative. More recent mainstream contractor failure and inflation and interest rate increases continue to put further pressure on their balance sheets, leading to a greater likelihood of failure.

Risk description	Update on risk status	Mitigation
<p>An insolvency of a key client, subcontractor, joint venture partner or supplier could disrupt project works, cause delay and incur the costs of finding a replacement, resulting in significant financial loss.</p> <div> <p>Change in risk</p>  <p>Responsibility The Board, Group management team, divisional senior management teams</p> <p>Strategic priority</p>  </div>	<ul style="list-style-type: none"> Supply chain insolvency risk has increased following some well-publicised failures in the mainstream contractor market. Where supply chain failures have occurred, they have been disruptive but manageable, with costs being absorbed at project level by utilising contingency and/or, in a small number of instances, a reduction in margin which has not been material to the Group. We have nurtured close relationships with our supply chain as part of a long-term strategy, sharing our values and desired behaviours, so that we can provide an offering our clients can rely on. We use supply chain credit checks but the information is somewhat historical. Our relationships with our suppliers mean we can monitor the situation in real time, by gaining transparency and understanding their levels of exposure, and our operational teams are highly alert to early signs of stress. This gives us a better chance of stepping in if needed. The strength of our balance sheet gives us the option of helping our supply chain partners manage short-term issues, such as cash flow, if and as deemed appropriate. Our strategy has been to reduce payment days and our supply chain partners regard us as dependable and responsible. In addition, we do not hold any cash in the form of retention from our preferred supply chain partners, which helps reduce their cash flow pressures and the likelihood of failure. 	<ul style="list-style-type: none"> Our business model and order book are predominantly focused on public sector and regulated industries and commercial customers in sound market sectors, reducing the likelihood of a material customer failure. We carry out rigorous due diligence preconstruction, particularly on commercial clients and key supply chain partners, including a focus on payment behaviours, cash terms and profiling, and likely liquidity outcomes. Mitigation could include obtaining, where necessary, relevant securities in the form of guarantees, bonds, escrows and/or more favourable payment terms, or, in some cases, declining a project. Formal due diligence is carried out when selecting joint venture partners, including seeking protection in the event of default by one of the partners. Joint ventures require executive director approval. We work with preferred or approved suppliers where possible, which aids visibility of both financial and workload commitments. Our business model reduces the concentration of supply chain risk as our divisions operate in different markets and geographical regions, using local supply chains. This helps ensure we do not overstress suppliers' finances or operational resources. Our predominant negotiated and two-stage procurement routes¹ allow us to select supply chain partners with optimal credentials tailored to each project, including qualitative, behavioural, resourcing and financial. This enables predictable outcomes for the Group, our clients and our supply chain. We rigorously monitor work in progress, debts and retentions.

Long-term scarcity of skilled labour in the industry

Issue/risk	Update	Comment/outlook
<p>This is a UK-wide issue which, while the sector works to broaden its appeal as a career option, will require considerable government and sector collaboration to resolve.</p> <p>This could impact our ability to deliver long-term growth and/or disrupt project delivery.</p> <p>It could lead to the ultimate resizing of the industry and the Group.</p>	<ul style="list-style-type: none"> We continue to manage some short-term issues, largely mitigated by our predominant two-stage procurement approach, which helps with longer-term labour resourcing and planning. Off-site, modular and new methods of construction help reduce on-site resource needs. Technology plays its part in reducing the need for site-based resource and attracting people into the industry but will require some upskilling to be undertaken. 	<ul style="list-style-type: none"> We engage with schools and local communities to encourage people to join the industry, and provide training and work opportunities. Our diversity and inclusion initiatives help make the industry more attractive and increase the talent pool. Our divisions' relationships with their supply chains help mitigate the effects of labour availability issues by sharing pipeline information and allowing long-term resource planning.

To help assess whether our principal risks are changing and remain within our appetite, the committee conducts deep dives into key areas. In 2024, the deep dives focused on:

- **supply chain liquidity** (see principal risk E, page 57), the committee noting that this risk had increased during the year due to industry failures and that it was important for the divisions to remain vigilant;
- **the effect of the economy on our residential portfolio** (see principal risk B, page 54), noting that while cost pressures were continuing to challenge the viability of some schemes, we have flexibility in our models to work through issues and seek alternative funding;
- **latent defects** (see principal risk I, page 60), the committee noting that this risk had reduced due to progress with remediation of building safety issues and a reduction in the likelihood of new issues arising, and agreeing to keep the Group's mitigating actions under review to ensure they remain appropriate; and
- **emerging risks** (see page 62), including longer-term potential scenarios that require monitoring.

Following its assessment at the year end, the committee noted that during 2024 our overall risk profile had stabilised, influenced by more resilient macro and consumer finances, easing of inflation and reduced cost-of-living pressures on households and businesses. The committee concluded that while some uncertainty continues, our risk profile has remained stable primarily because our markets are predominantly in the public and regulatory sectors. The committee regards these sectors to be structurally secure and noted that they include recent government commitments to critical construction and infrastructure such as affordable housing and regeneration which align to the Group's strategy. More detail on challenges in our markets and how we are mitigating them can be found in our market conditions section on page 16 and in our managing risk section on pages 54 and 57 (principal risks A, B and E respectively).

Figure 29

British Land FY25 ARA, p. 50-51, 57

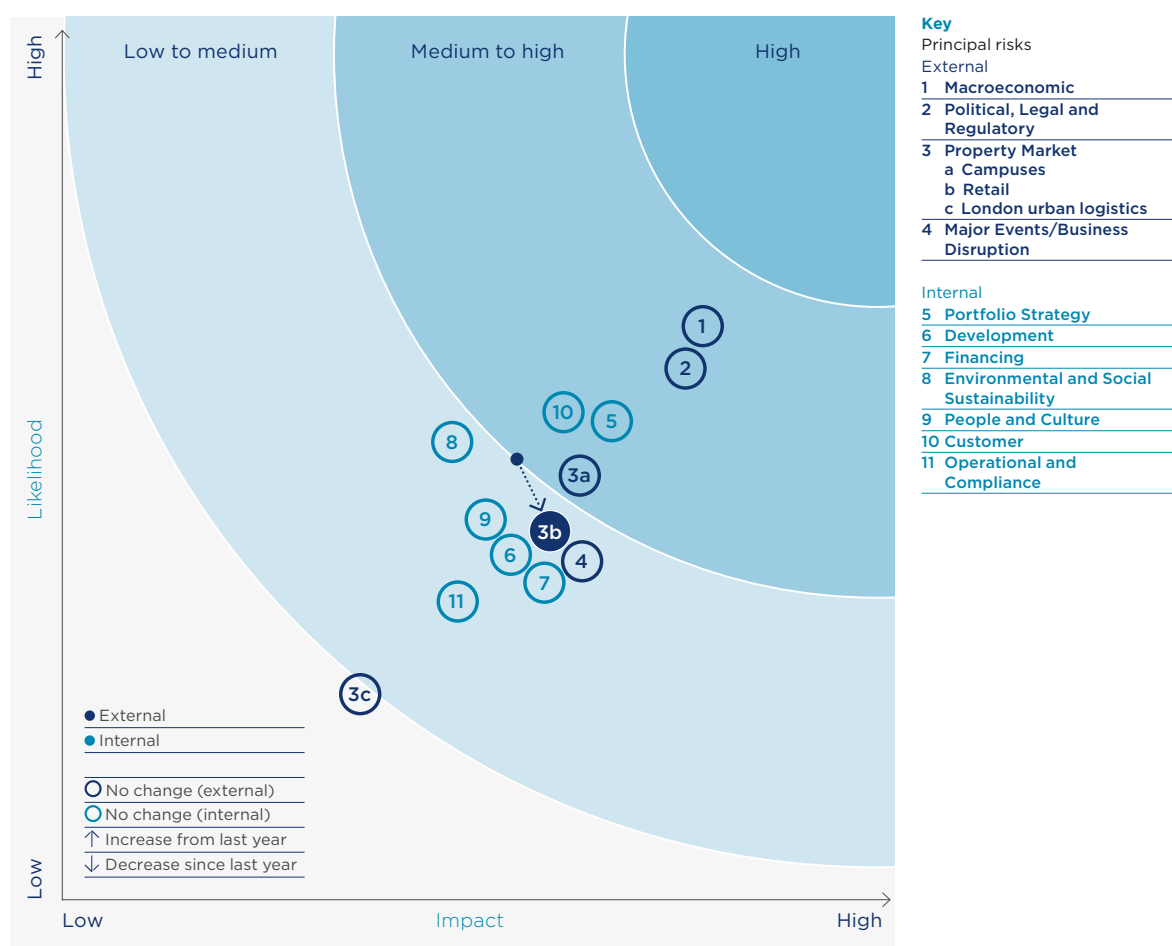
Our principal risks

Our risk management framework is structured around the principal risks facing British Land. Using a risk scoring matrix, we assess risks based on likelihood, financial impact and reputational impact. This process aids in identifying both the external and internal strategic and operational principal risks with a higher likelihood and potential impact on our business.

Our principal risks comprise the 11 most significant Group risks, including four external risks primarily influenced by market factors, and seven internal strategic and operational risks which, while subject to external influence, are more under the control of management. External principal risks stem from the broader macroeconomic and political environment, as well as our core property markets.

Internal principal risks relate to our capital allocation, development, customers, sustainability, people and culture, as well as key operational risks such as technology, health and safety, and fraud and compliance. The Board, supported by the Audit Committee conducts regular reviews of external principal risks to inform decision making, while internal risks are managed through strong governance, controls and operational processes.

Risk heat map



Note: The above illustrates principal risks which by their nature are those which have the potential to significantly impact the Group's strategic objectives, financial position or reputation. The heat map highlights net risk, after taking account of principal mitigations. The arrow shows the movement from 31 March 2024.

10 Customer

Link to strategy:
A B C D

The Group’s primary source of income is rent received from our customers. This could be adversely affected by non-payment of rent; occupier failures; evolving customer needs; leasing challenges; poor customer service; and potential changes in lease structures.

Risk mitigation

- **Diversified Customer Base:** Maintain a high quality, diversified occupier base to mitigate individual occupier risks.
- **Occupier Strength and Robust Rent Collection:** Conduct thorough covenant checks before deals and ongoing monitoring, with a risk watchlist reviewed by the Risk Committee. We proactively limit financial exposure to high risk occupiers.
- **Occupier Engagement and Market Knowledge:** Work closely with occupiers to understand and meet their evolving requirements.
- **Portfolio Leverage and Active Asset Management:** Strategically address lease breaks and expiries to maintain high occupancy and minimise vacancies.
- **Customer Satisfaction:** Regular surveys assess occupier experience and service levels.

Risk assessment

Our overall customer risk remains broadly stable, supported by strong

rent collection and robust leasing activity. While there has been an increase in retailer administrations and restructuring plans in the market, we have proactively limited their financial impact.

Emerging risk trends:

- Macroeconomic and geopolitical volatility, including the impact of new global tariffs
- Evolving work patterns (e.g. hybrid working)
- AI and emerging technologies
- Budget NI increases

Opportunity/approach

Successful customer relationships are critical to our business growth. Our business model revolves around our customers. Our strategic positioning across campuses, retail parks and London urban logistics, along with strong collaborative relationships, is focused on providing high quality spaces, while maintaining sustainable occupancy costs.

Impact:

Medium

Likelihood (post-mitigation):

Medium

Change in risk assessment in year:


Risk appetite:
Balanced

KRIs

- Market letting risk, including vacancies, upcoming expiries and breaks and speculative development
- Occupier covenant strength and concentration (including percentage of rent classified as ‘High Risk’ and affected by insolvencies)
- Occupancy and weighted average unexpired lease term
- Rent collection

Overseen by:
Head of Real Estate and Investments and CFO

Source: British Land Annual Report and Accounts 2025

Figure 30




Glencore 2024 ARA, p. 92

1. Supply, demand and prices of commodities		
2024 vs. 2023	Risk appetite	Link to strategy
	Cautious	

We are subject to the inherent risk of sustained low prices for our main commodities, particularly affecting our industrial business. The revenue and earnings of substantial parts of our industrial asset activities and, to a lesser extent, our marketing activities, are dependent upon prevailing commodity prices. The prices of the commodities we produce are dependent on the expected volumes of supply or demand for commodities which can vary for many reasons out of our control.

New or improved energy production possibilities and/or technologies are likely to reduce the demand for some commodities. Governmental net zero emissions targets will require demand for unabated thermal coal and other hydrocarbon fuel sources to significantly reduce over time.

The dependence of the Group (especially our industrial business) on commodity prices, supply and demand of commodities, makes this the Group's foremost risk.

Strategic priorities	
	Responsible and ethical business practices
	Effective capital management
	Strong operational and commercial performance

Potential impact on the Group

- Significant falls in the prices of certain commodities (e.g., copper and coal) can have a severe drag on our financial performance, impede shareholder returns and could lead to concerns by external stakeholders as to the strength of the Group's balance sheet.
- A global surplus or shortage in one or more of the commodities we produce could have a major impact on their price, and therefore on our financial performance.

Mitigating factors or controls

Inherent business model mitigations:

- We maintain a diverse portfolio of commodities, geographies, assets and contracts.
- We seek to prepare for anticipated shifts in commodity demand, for example by prioritising investment in parts of the business that will potentially grow with increases in renewable energy generation and EVs and battery production, and by closely monitoring fossil fuel (particularly thermal coal) demands. We are also able to reduce the production of commodities within our portfolio in response to changing market conditions.

Established and implemented mitigating controls:

- Our financial leverage of under 1x in the ordinary course of business should support our ability to obtain financing in a downside scenario (see *Liquidity* on page 98).
- We continue to maintain focus on cost discipline and achieving greater operational efficiency to increase our resilience to lower prices.
- We actively manage commodity price risk in our marketing segment, including via daily analysis of Group VaR.

Source: <https://www.glencore.com/.rest/api/v1/documents/static/7a4295e4-3674-45e9-94c4-7d7fb285faff/GLEN-2024-Annual-Report.pdf>

Figure 31

IHG 2024 ARA, p. 47

Owner preferences for, or ability to invest in, our brands

Why this uncertainty is important to the achievement of our strategic objectives over the next 2–3 years

Our growth ambitions require us to take calculated risks to attract owners while continuing to drive returns for our existing and potential owners.

Continuing macroeconomic uncertainty and inflation create significant pressures on owners' financial capacity that must be considered carefully as we pursue opportunities to drive brand preference and focus on relentless growth.

These opportunities need to be balanced with the risks associated with increasingly complex deal structures, new strategic relationships, expansion into new markets and a need to risk our own capital to pursue inorganic growth or to incentivise deals in key locations for key brands. We also recognise our responsibilities as a franchisor and manager of our brands.

If we fail to respond effectively to this risk, we will lose competitiveness and may not realise the opportunities to grow our brand footprint.

Executive Risk Sponsor

- Global Chief Commercial and Marketing Officer
- Regional CEOs

Link to strategy



Example factors discussed with management to monitor trending

- Owner financial capacity (current and future), including continuing the impact of macroeconomic uncertainties.
- Preference for and confidence in IHG's enterprise platforms.
- IHG's ability to drive bottom line returns and preference for existing and potential owners, relative to competition.
- Overall owner advocacy and relationship strength, gathered through feedback from owners.

Illustrative key controls

Culture and leadership:

- IHG masterbrand, loyalty and individual brand strategies.
- Governance structures and leadership responsibilities to monitor owner returns and support owner finance.
- Colleague training on drivers of loyalty and owner returns.

Processes and controls:

- Specific projects focused on owner returns (including sustainability, procurement, hotel technology, learning).
- Brand development processes with ROI targets.
- Compliance processes, including Guest Love and quality evaluations.

Monitoring and reporting:

- Regular tracking of cost to build, open and operate hotels.
- Key Executive Committee metrics on Growth and Enterprise, and Loyalty contribution.
- Tracking of external data and competitor analysis.
- Measurement of ongoing performance and strategy delivery.

Examples of how the Board obtained assurance on our risk management and resilience in 2024

- Priority market updates from regional CEOs.
- Review of new brand, partnership and key owner-facing technology initiatives.
- Review of System Fund and loyalty programme changes.
- Review of energy, water and waste strategies.
- The Internal Audit plan included independent assurance on governance for the Low Carbon Pioneers programme and data integrity for key owner metrics.



For further information on why hotel owners choose to work with IHG see page 27.

Figure 32

United Utilities FY25 ARA, p. 57, 59

Our principal risks

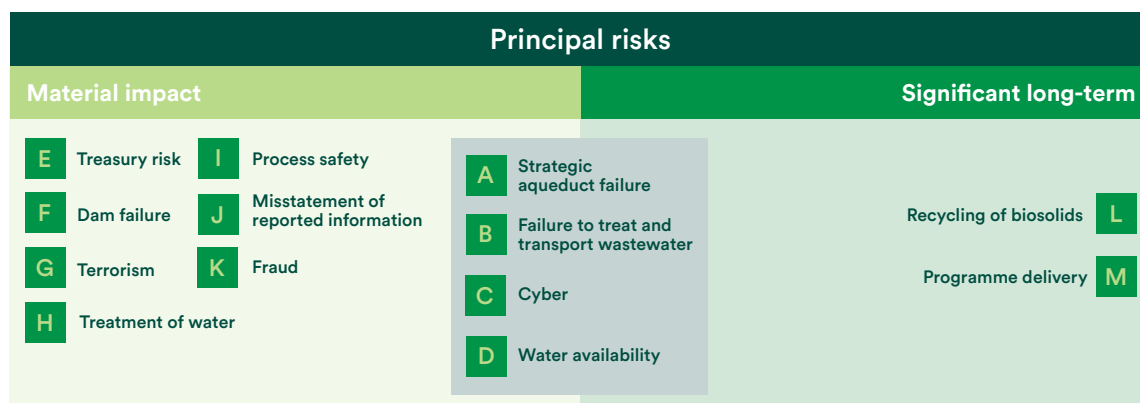
In January 2024, the FRC published a revised UK Corporate Governance Code (the code), with the most significant change being in respect of Provision 29, which relates to the board monitoring the risk management and internal control framework. In accordance with the revised code, the board will make a declaration of the effectiveness of material controls from financial year 2026/27, which will supplement the existing annual assessment of risk management and internal control systems (see pages 124 to 125 in our integrated annual report). As we take steps in preparation for the material controls declaration, we have renewed our definition of which event-based risks, individually or collectively, are to be considered as a principal risk:

- Material impact risks – risks, which in the maximum worst case, have severe one-off financial and non-financial impacts; and/or
- Significant long-term risks – risks with significant exposure (likelihood of occurrence of the event multiplied by the most likely financial impact over the long term after consideration of the current control environment).

Our principal risks, therefore, represent those risks, which, in a remote but plausible scenario, could initiate corporate failure (material impact risks) and those risks that are likely to have a significant long-term impact on company value if they were to crystallise. As our definition of material impact risks highlights those risks that have the most significant impact (if they crystallise in the worst case), it naturally identifies risks

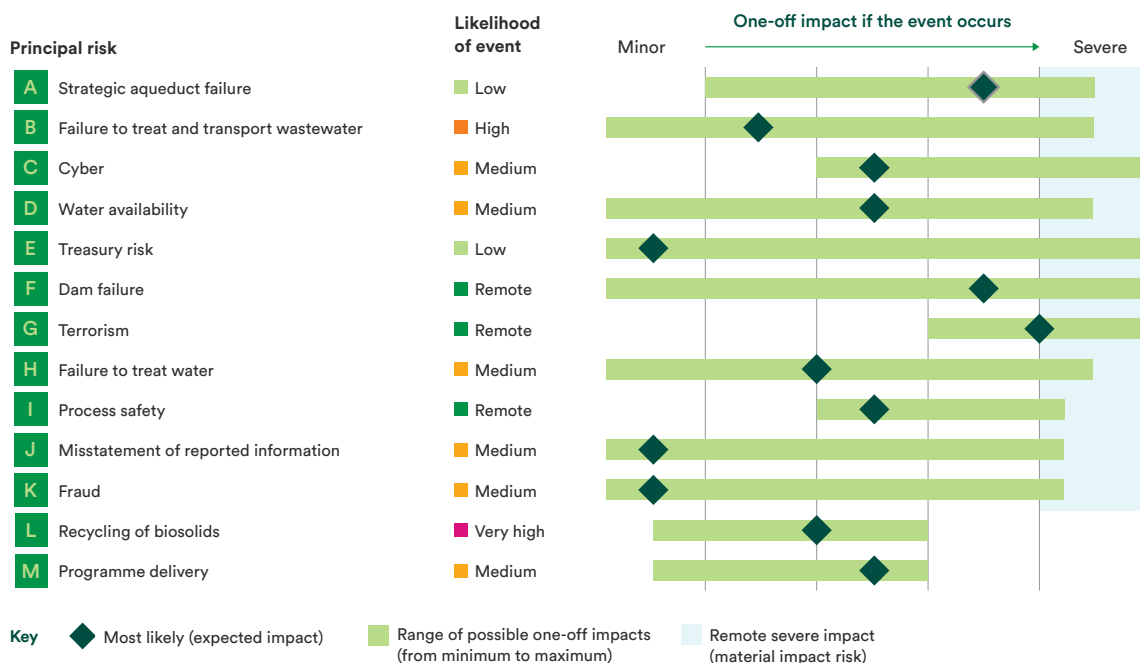
which place significant reliance on mitigating controls. Therefore, our future material controls declaration will be in respect of the key controls which mitigate our material impact risks.

The overlap between the material impact and significant long-term risks is represented in the diagram below. A summary of the principal risks and associated mitigation/control is provided on pages 58 to 59.





Principal risk exposure

The bar chart below illustrates the likelihood of each event-based risk occurring (relative to its causal factors) and the indicative full range of potential one-off financial impacts (from minimum to maximum) should the risk materialise. Each of the multiple impacts in the range is subject to an individual post event probability, the most likely of which is illustrated by the diamond. Where the remote maximum impact is both financially and non-financially severe (as highlighted by the blue box), it is regarded as being material, constituting a material impact risk.



Principal risk	Risk exposure	Control/mitigation	Governance and assurance
 ↔ Treatment of water  	Threats to water treatment include asset health, process failure and the contamination (natural, chemical or biological) of raw water. Climate change is a key factor of raw water contamination due to intensifying catchment erosion and runoff, more frequent wildfires and increasing algal bloom, which can produce taste and odour problems. Failure to treat water can lead to non-compliance with regulatory standards, rejection of water by consumers for aesthetics or, in extreme cases, public health issues.	<p>We are committed to providing wholesome drinking water. Material controls are:</p> <ul style="list-style-type: none"> • Sampling and testing: Occurs across the entire system to ensure water is safe and compliant. • Sensors and alarms: Monitors deviations from acceptable levels with alarm triggered response. • Maintenance: Inspection, servicing, repair and replacement of assets due to proactive and reactive activity. • Licence to operate: Training and competence. <p>Other controls include an end-to-end risk assessment process, contingency plans, and the monitoring of the regulatory position on emerging contaminants.</p>	<p>Governance</p> <ul style="list-style-type: none"> • Water quality first board^M • Water price control^M <p>Assurance</p> <ul style="list-style-type: none"> • Scientific service team reviews² • Assurance team reviews² • Cyclical internal audits³
 ↔ Process safety 	Our activities include chemical, biological and physical processes that are inherently hazardous, with the storage of toxic and explosive gases across multiple sites (two of which fall under the Control of Major Accident Hazard (COMAH) regulations). An unintentional release of chemicals, energy, or other potentially dangerous materials (including steam) during these day-to-day activities could, in the worst case, have a serious effect on people, plant/equipment, and the environment.	<p>We are committed to improving health and safety performance, with process safety being a primary area of focus. Material controls are:</p> <ul style="list-style-type: none"> • Control of work: A management system that includes authorisation, isolation and permit to work. • Management of change: Risk assessment and safe, effective implementation of changes. • Maintenance: Inspection, servicing, repair and replacement of assets due to proactive and reactive activity. • Licence to operate: Training and competence. <p>Other controls include monitoring through sensors and alarms and emergency/contingency plans.</p>	<p>Governance</p> <ul style="list-style-type: none"> • Process safety group^M • Health & safety board^M <p>Assurance</p> <ul style="list-style-type: none"> • H&S team reviews² • Assurance team reviews² • Cyclical internal audit³
 ↔ Misstatement of reported information 	We are bound by legislation and regulation to provide statutory financial accounts and regulatory reports to demonstrate financial health, performance, compliance with legal and regulatory requirements, and provide information to stakeholders for their ongoing interest and/or investment in the company. Failure to provide accurate and/or complete information is reputationally damaging and, depending on the nature of any misstatement or misreport, could accrue significant penalties and additional scrutiny.	<p>We are committed to reporting in an open, compliant and transparent way. Material controls are:</p> <ul style="list-style-type: none"> • Financial controls: A management system including journal procedures, analytical reviews, and control accounts. • Regulatory reporting framework: A set of principles relating to reporting criteria, accountabilities, data capture, governance and assurance. • Validation: The identification of potential errors and reconciliation of financial parameters. <p>Other controls include accounting policies, schedules, risk assessment and management of queries.</p>	<p>Governance</p> <ul style="list-style-type: none"> • Executive performance meetings^M • Audit committee⁸ • Compliance committee⁸ <p>Assurance</p> <ul style="list-style-type: none"> • Financial control team review² • Regulation and compliance team review² • Internal audits³ • External audit³
 ↔ Fraud 	The scale of UU's operations presents multiple opportunities for fraud to be perpetrated from inside and outside of the company, potentially impacting us, our stakeholders and third parties. Fraud can be committed by individuals or groups with examples including false representation, unauthorised disclosure of personal information, the supply of inferior products / false invoices, and misuse or theft of company property. The Economic Crime and Corporate Transparency Act 2023 introduced a new corporate offence for failure to prevent fraud, which can carry an unlimited fine.	<p>We are committed to preventing fraud. Material controls are:</p> <ul style="list-style-type: none"> • Control of work: A management system that includes authorisation, delegated authority, segregation of duties, supervision and data protection procedures. • System access controls: Restrictions to systems, data and internet usage. • Procurement & purchasing standards: Strict procedures to procure services and purchase goods. • Verification: Checks on invoices, bills and refunds. <p>Other controls include awareness training, confidential reporting and a fraud risk assessment.</p>	<p>Governance</p> <ul style="list-style-type: none"> • Security steering group^M • Whistleblowing committee^M • Audit committee⁸ • Group board⁸ <p>Assurance</p> <ul style="list-style-type: none"> • Departmental review² • Cyclical internal audit³ • External review³
 ↑ Recycling of biosolids  	Wastewater treatment generates significant quantities of sludge, which is subsequently treated to produce biosolids, the majority of which are recycled to agriculture as the most practical environmental option. A reduction in the landbank could have significant implications to strategy and operations with a total loss being the worst-case scenario. Threats include: the quality of biosolids; changes in public or political perception; changes in regulations associated with emerging contaminants and climate change; and/or the willingness of farmers or landowners to receive biosolids.	Treatment, sampling and testing ensures that quality standards are met, and we work closely with farmers, landowners and contractors to ensure compliance with regulations (notably the Biosolids Assurance Scheme). We are also investing in our sludge treatment assets to ensure capacity, reliability and environmental compliance is upheld. In addition, we continue to work closely with regulators to influence policy. We are also developing contingency plans should regulation change in the near term, with a notified item included in the final determination enabling an interim determination (IDOK) if significant investment is required to develop alternative disposal outlets before 2030.	<p>Governance</p> <ul style="list-style-type: none"> • Bioresource team review of BAS compliance^M • Executive performance meetings^M <p>Assurance</p> <ul style="list-style-type: none"> • Assurance team reviews² • Cyclical internal audit³ • External BAS audits³
 ↑ Programme delivery 	The capital programme involves significant investment in the development and improvement of point and linear assets through a series of projects to improve water supply and wastewater services. Delivery to time, cost and quality is under constant challenge due to ongoing exposure to natural hazards and the capacity and capability of third parties, partners and internal resource. This risk is amplified by the significant scale of the capital programme across this and future asset management periods (AMPs) coupled with challenging cost allowances and performance commitments.	Our capital programme operating model involves multiple construction and design partners, and a large supplier base, providing both efficiency and resilience. With strong emphasis placed on safety and the environment, we adopt a supplier relationship management framework to manage contracts and performance, a runway approach for project allocation, and category management for the supply of products and materials. Performance is measured through our capital programme delivery incentive and monitoring performance commitment deliverables. For operations, a transformation programme is in development with five clear areas of focus within an agreed prioritisation framework.	<p>Governance</p> <ul style="list-style-type: none"> • Project management office^M • Capital investment committee^M • Executive performance meetings^M <p>Assurance</p> <ul style="list-style-type: none"> • Assurance team reviews² • Cyclical internal audit³

Key	Risk Categorisation	Governance	Assurance (refer to pages 139 to 141 in our integrated annual report)
	 Material impact  Significant long-term exposure	M Management committee B Board committee	2 Second line assurance activity 3 Third line assurance
	Change in risk exposure over the year (see page 60 for explanation)		
	↔ Stable ↑ Increased		

Source: [32631-united-utilities-sr-2025-200625.pdf](#)

Figure 33

Bunzl 2024 ARA, p. 97

RISK MANAGEMENT AND INTERNAL CONTROLS OVERVIEW

The Board has delegated to an Executive Committee, consisting of the CEO, CFO and other functional managers, the initial responsibility for identifying, evaluating, managing and mitigating the risks facing the Group and for deciding how these are best managed, as well as responsibility for establishing a system of internal controls appropriate to the business environments in which the Group operates. The principal features of this system include:

- a procedure for monitoring the effectiveness of the internal controls system through a tiered management structure with clearly defined lines of responsibility and delegation of authority;
- a second line of defence Internal Controls team to continually develop the Group's framework and approach to internal controls over financial reporting;
- formal standards of business conduct (including code of conduct, anti-bribery and corruption, fraud investigations and reporting, and whistleblowing policies) based on honesty, integrity, fair dealing and compliance with the local laws and regulations of the countries in which the Group operates;
- strategic plans and comprehensive budgets which are prepared annually by the business areas and approved by the Board;
- clearly defined authorisation procedures for capital investment and acquisitions;
- a well-established consolidation and reporting system for the statutory accounts and monthly management accounts;
- detailed manuals covering Group accounting policies, and policies and procedures for the Group's treasury operations supplemented by internal controls procedures at a business area level;
- periodic IT risk assessment aligned with the Group's IT security standard, as well as continual investment in IT systems and security to ensure the security of information systems and data, business continuity and the production of timely and accurate management information; and
- considering ESG and non-financial reporting and assurance.

Some of the procedures carried out in order to monitor the effectiveness of the internal controls system and to identify, manage and mitigate business risk are:

- central management holds regular meetings with business area management to discuss strategic, operational and financial issues, including a review of the principal risks affecting each of the business areas and the policies and procedures by which these risks are managed;
- the Executive Committee reviews the outcome of the discussions held at business area meetings on internal controls and risk management issues;
- the Board in turn reviews the outcome of the Executive Committee discussions on internal controls and risk management issues, which ensures a documented and auditable trail of accountability;
- each business area, the Executive Committee and the Board carry out an annual fraud risk assessment. Reporting protocols are in place to identify, analyse and respond to actual or potential fraud incidents;
- an annual self-assessment of the status of internal controls measured against a prescribed list of minimum standards is performed by every business and action plans are agreed where remedial action is required;
- actual results are reviewed monthly against budget, forecasts and the previous year and explanations are obtained for all significant variances;
- all treasury activities, including in relation to the management of foreign exchange exposures and Group borrowings, are reported and reviewed monthly. The Group's bank balances around the world are monitored on a weekly basis and significant movements are reviewed centrally;

- developments in tax, treasury and accounting are continually monitored by Group management in association with external advisers;
- regular meetings are held with insurance and risk advisers to assess the risks throughout the Group;
- systems are in place to monitor IT security incidents, analyse them and remediate any identified weaknesses. Findings are used to continually improve defences across all Group companies;
- the Internal Audit function periodically performs business and risk-themed audit work, makes recommendations to improve processes and controls and follows up to ensure that management implements the recommendations made. The Internal Audit function's work is determined on a risk assessment basis and its findings are reported to Group and business area management as well as to the Audit Committee and the external auditors;
- the Audit Committee, which comprises all of the independent non-executive directors of the Company, meets regularly throughout the year. Further details of the work of the Committee, which includes a review of the effectiveness of the Company's internal financial controls and the assurance procedures relating to the Company's risk management system, are set out in the Audit Committee report on pages 102 to 111;
- management committees (known as the Group Sustainability Committee, the Environment & Climate Change Committee, the Health & Safety Committee, and the Supply Chain Committee) which oversee issues relating principally to environment, health & safety and business continuity planning matters, set relevant policies and practices and monitor their implementation; and
- health & safety risk assessments, safety audits and a regular review of progress against objectives established by each business area are periodically carried out.

Source: https://www.bunzl.com/media/zrapvmdv/bunzl_ar24_interactive.pdf

Figure 34

IWG 2024 ARA, p. 70

On the request of the Board the Committee monitors the Group's implementation of its sustainability policies. In respect of 2024, this included reviewing the limited assurance work performed by an independent third party on our Scope 1 and 2 greenhouse gas emissions information included on page 44, as well as the Committee's assessment of the impact of climate related risks on the Group's financial statements as detailed in note 2 on page 102. The Committee also reviewed the disclosures provided on pages 41 to 43 in compliance with the framework provided by the Task Force on Climate-Related Financial Disclosures.

Internal control

The Committee has a delegated responsibility for the Company's system of internal control and risk management and for reviewing the effectiveness of this system. Such a system is designed to identify, evaluate and control the significant risks associated with the Group's achievement of its business objectives with a view to safeguarding shareholders' investments and the Group's assets. Due to the limitations that are inherent in any system of internal control, this system is designed to meet the Group's particular needs and the risks to which it is exposed and is designed to manage rather than eliminate risk. Accordingly, such a system can provide reasonable, but not absolute, assurance against material misstatement or loss.

In accordance with the FRC's Guidance on Risk Management, Internal Control and Related Financial and Business Reporting (the 'FRC Guidance'), the Committee confirms there is an ongoing process for identifying, evaluating and managing significant risks faced by the Group.

During 2024, the Committee continued to revisit its risk identification and assessment processes, inviting Board members and senior management to convene and discuss the Group's key risks and mitigating controls.

A risk-based approach has been adopted in establishing the Group's system of internal control and in reviewing its effectiveness. To identify and manage key risks:

- Group-wide procedures, policies and standards have been established;
- a framework for reporting and escalating significant matters is maintained;
- reviews of the effectiveness of management actions in addressing key Group risks identified by the Board have been undertaken; and
- a system of regular reports from management setting out key performance and risk indicators has been developed.

This process is designed to provide assurance by way of cumulative assessment and is embedded in operational management and governance processes.

Key elements of the Group's system of internal control which have operated throughout the year under review are as follows:

- the risk assessments of all significant business decisions at the individual transaction level, and as part of the annual business planning process;
- a Group-wide risk register is maintained and updated at least annually whereby all inherent risks are identified and assessed, and appropriate action plans developed to manage the risk per the risk appetite of the Group as established by the Board. The Board reviews the Group's principal risks at least annually and management periodically reports on the progress against agreed actions, enabling the Committee to monitor how key risks are managed;
- the annual strategic planning process, which is designed to ensure consistency with the Company's strategic objectives. The final plan is reviewed and approved by the Board. Performance is reviewed against objectives at each Board meeting;
- comprehensive monthly business review processes under which business performance is reviewed at business line, business centre, area, country, regional and functional levels. Actual results are reviewed against targets, explanations are received for all material movements, and recovery plans are agreed where appropriate;
- the documentation of key policies and control procedures (including finance, operations, and health and safety) having Group-wide application.

These are available to all staff through the IWG Academy;

- formal procedures for the review and approval of all investment and acquisition projects. The Group's Investment Committee reviews and approves all investments. Additionally, the form and content of routine investment proposals are standardised to facilitate the review process;
- the delegation of authority limits with regard to the approval of transactions;
- the generation of targeted, action-oriented reports from the Group's sales and operating systems on a daily, weekly and monthly basis, which provide management at all levels with performance data for their area of responsibility, and which help them to focus on key issues and manage them more effectively;
- the delivery of a centrally coordinated assurance programme by the business assurance department that includes key business risk areas. The findings and recommendations of each review are reported to both management and the Committee; and
- the maintenance of high standards of behaviour which are demanded from staff at all levels in the Group. The following procedures support this:
 - a clearly defined organisation structure with established responsibilities;
 - an induction process to educate new team members on the standards required from them in their role, including business ethics and compliance, regulation and internal policies;
 - the availability of Group and country-specific policies via the Group's internal platforms, including the Company's Code of Conduct, detailed guidance on employee policies and the standards of behaviour required of staff;
 - policies, procedure manuals and guidelines are readily accessible through the IWG Academy;
 - operational audit and self-certification tools which require individual managers to confirm their adherence to Group policies and procedures; and
 - a Group-wide policy to recruit and develop appropriately skilled employees of high calibre and integrity and with appropriate disciplines.

The Committee and the Board regard responsible corporate behaviour as an integral part of the overall governance framework and believe that it should be fully integrated into management structures and systems. Therefore, the risk management policies, procedures and monitoring methods described above apply equally to the identification, evaluation and control of the Company's safety, ethical and environmental risks and opportunities. This approach makes sure that the Company has the necessary and adequate information to identify and assess risks and opportunities affecting the Company's long-term value arising from its handling of corporate responsibility and corporate governance matters.

The Committee has completed its annual review of the effectiveness of the system of internal control for the year to 31 December 2024 and is satisfied that it is in accordance with the FRC Guidance and the Code. The assessment included consideration of the effectiveness of the Board's ongoing process for identifying, evaluating and managing the risks facing the Group.

Whistleblowing policy

A whistleblowing channel, hosted by an independent third party and which may be used anonymously, is available to all employees via email, the web, or on the IWG Academy. We operate a 'Right to Speak' policy, the aim of which is to encourage all employees, regardless of seniority, to bring matters that cause them concern to the attention of the Committee, through the whistleblowing channel, without fear of repercussions or retaliation. Employees can monitor the progress of the reports they have made.

The Business Assurance Director, in consultation with the Senior Leadership Team, decides on the appropriate method and level of investigation. The Committee is notified of all material discourses made and receives reports on the results of investigations and actions taken on a regular basis. The Committee has power to request further information, conduct its own enquiries or order additional action as it sees fit.

Figure 35

Spire Healthcare 2024 ARA, p. 67-68

Internal controls

1) Standard policies and procedures

We have documented policies and standard procedures in place covering all significant activities and areas of risk, which are subject to regular review and update by the policy approval committee (PAC) comprising a cross functional membership of subject matter experts. The PAC reports into the safety, quality and risk committee. The PAC meets eleven times a year and publishes updates to policies on our intranet. All policies are required to follow a standard process for creation and review. There is a standard structure for procedures and guidelines to provide our colleagues and consultants with further operational detail for policies where required. The default review period once a policy is approved is three years but can be shorter if required. There are certain policies that the board reserves the right to approve, for example treasury management, raising concerns and risk management policies.

2) Assurance over clinical delivery and clinical regulatory compliance risks

As a provider of clinical services to patients, we face a specific set of non-financial risks associated with such provision. We have strong control structures as described below.

- The group medical director oversees the governance of the medical professional standards of 8,740 consultants through the medical professional standards committee, the management of patient reviews and recalls, the processes for the management of practising privileges and setting medical governance policy
- The integrated quality governance team supports a suite of clinical audits which assess compliance with key areas of patient safety
- In 2024, two major improvements to the clinical quality control framework were rolled out. First, in January 2024, we issued the new group wide integrated quality governance structure for Spire Hospitals. Second, in March 2024, we rolled out the new Patient Safety Incident Response Framework (PSIRF) (see page 26)
- The central clinical team oversees a national programme of clinical reviews including testing, according to the approach taken at regulatory inspections
- The central clinical team also oversees the drafting, communication and training of a comprehensive set of clinical policies and procedures for Spire Healthcare. These form part of the overall framework for clinical safety governance and quality, to ensure that clinical risk and clinical regulatory compliance is managed effectively across all registered sites. The governance activities are monitored by the integrated quality governance team and are reported regularly to the safety, quality and risk committee, the executive committee and the clinical governance and safety committee
- Each hospital has a risk register through which clinical and medical risks are managed, mitigated and escalated
- Comprehensive, non-financial management information on quality including safety, clinical effectiveness and patient experience is produced and reviewed monthly against pre-agreed standards by the corporate integrated quality governance and clinical teams and reported to the safety quality and risk committee sub-committee bi-monthly and reported to the clinical governance and safety committee quarterly
- We are subject to substantial levels of external inspection and review, both by the range of national healthcare regulators (CQC/HIW/HIS), and through invited assurance inspections such as the rolling programme of health and safety inspections carried out by third-party specialists. The executive committee and the clinical governance and safety committee review the outcomes of these activities. In 2024, we had a total of four CQC and HIW/HIS inspections, all producing 'Good', 'Outstanding', or equivalent performance assessments
- We have maintained throughout 2024 the structures and processes to provide the level of evidence and assurance required to monitor clinical regulatory compliance

3) Financial and operational controls

Our design of our finance function splits resources across on-site finance directors at each hospital, supported by a central finance function based in Reading.

We received regular fraud updates from the NHS Counter Fraud Authority during the year and, where relevant, disseminated the fraud alerts to relevant colleagues. We were subject to daily direct and indirect cyber-attacks during the year. We have prepared response plans to cyber-attacks utilising both in-house and third-party experts. After any incident, we undertake a full incident review and reflect learnings into our cyber-security environment.

The fundamental financial controls as reported in 2023 remained in place during 2024, namely:

- The annual process of preparing business plans and budgets, followed up by close monitoring of operational performance by the executive committee and the board
- Weekly forecasting and actual reviews to drive corrective actions
- Monthly monitoring of actual results, compared to budgets, forecasts and the previous year
- All material capital, leasing and acquisition projects are subject to an investment evaluation and authorisation procedure, including board approval, when the forecast expenditure exceeds the level of delegated authority
- Common accounting policies and procedures
- Our cash flow position is regularly reviewed to ensure that our borrowings are aligned with our growth. Half yearly detailed cash flow forecasts are reviewed and used for controls over going concern, goodwill impairment and banking covenant assessments
- Forced segregation of duty and senior review of all payments made
- Other non-financial operational risks are managed by means of the application of best practice, as defined by group policies and standard procedures, in areas such as project management, human resources management and IT security and delivery, supported by detailed performance monitoring of outputs and issues
- Consolidation of our accounts bi-annually for accurate reporting purposes
- Key account balance sheet reconciliations to ensure accuracy within our accounts

Other non-financial operational risks are managed by means of the application of best practice, as defined by group policies and standard procedures, in areas such as project management, human resources management and IT security and delivery, supported by detailed performance monitoring of outputs and issues.

The Financial Reporting Council published the 2024 Corporate Governance Code requiring new disclosures over our risk management and internal control environment for our fiscal year starting 1 January 2026. We continue to prepare for these new requirements by documenting and strengthening our internal financial controls where appropriate.

4) Internal Audit

An in-house director of internal audit was supported by a dedicated team from KPMG who provide co-source internal audit resource. From 2025, this service has moved to RSM. The activities of internal audit are reported in the audit and risk committee report on pages 105 to 110.

Figure 36

Intertek 2024 ARA, p. 2.58, 2.92

Internal control and risk management systems

The Board ultimately reviews the Group's risks, controls and compliance and mitigation actions. The Committee is responsible for reviewing the adequacy and effectiveness of that risk framework. We have an integrated approach to obtaining assurance that our risks are being appropriately and effectively identified and addressed. Further information on how Intertek has implemented an end-to-end integrated approach to risk, control and compliance is outlined on pages 1.57-1.59 in Report 1.

'Doing Business the Right Way' is at the heart of what we do and continues to be a key enabler of our AAA strategy. The Intertek CMCs are an integral part of 'Doing Business the Right Way', and provide the mechanism by which we define, monitor and achieve consistently high standards in our control environment throughout the whole organisation. At the end of the year, the Committee undertook a review of the effectiveness of the CMCs and Assurance Map to ensure that they continued to be fit for purpose. Where non-compliances with the current CMCs were identified in the 2024 internal audit review process, remediation plans have been put in place. For 2025, the effectiveness of the process was reviewed and there were additional controls introduced based on risks and issues highlighted by the Group's Internal Audit and Compliance assurance programmes and based on other risk indicator data and outputs including the reporting, review and corrective actions of Hotline reports.

In order to provide assurance that the Intertek controls and policy framework is being adhered to, a self-assessment exercise is undertaken across the Group's global operations. This exercise is reviewed and refreshed each year to align with the updated control framework and to support the continued development of the Group's control environment.

Relevant operational and functional leaders for each site are required to complete a year end compliance certification, in the form of an online questionnaire, to confirm that the right management processes and controls are in place and are operationally effective. The compliance certification covers all CMC areas: Compliance, Sales, Operations, Marketing, Communications, our use of intermediaries, IT, Finance, Sustainability and People management. Where corrective actions are needed, the leaders are 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 2025.

Self-assessment responses are consolidated for review at a divisional, regional and functional level, with further review and sign-off of the consolidated self-assessments in the corresponding divisional, regional and functional 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 expanded during the year to ensure global coverage and to reflect Intertek's operational and financial structure, and in order to enhance the alignment of the self-assessment to the assurance process.

We annually review and approve the statements to be included in the Annual Report & Accounts to ensure they remain relevant to the Group's strategy and operations as well as complying with any regulatory requirements. A detailed verification programme also provides assurance to the Committee and the Board when checking that all the statements made in the Annual Report & Accounts are accurate. Intertek's Manual of Accounting Policies and Procedures is issued to all finance staff giving instructions and guidance on all aspects of accounting and reporting that apply to the Group.

The Committee can confirm that it reviewed the Group's internal controls and risk management systems and concluded that there was an effective control environment in place across the Group during 2024, and up to the date on which these financial statements were approved. No significant failings or weaknesses were identified.

In action

New risk committee structure

In a dynamic and constantly changing world, our products and services are always evolving to meet the needs of our stakeholders. This means that we are continuously reviewing and refreshing our approach to 'Doing Business the Right Way' – our internal risk, control, compliance and quality programme.

Through our integrated approach to risk management, we have regional, divisional and functional committees reporting to a Group Risk Committee, which manages, assesses and promotes the continuous improvement of our risk management, controls and assurance systems. Having adjusted our business model to report revenue, operating profit and margin across five divisions in 2023, we aligned our risk committee governance structure to support risk management in these divisions during 2024.

As we have welcomed many new colleagues since the launch of 'Doing Business the Right Way' in 2017, we also took the opportunity to refresh and set expectations for all risk committee members around the world. This included training on our processes and further reviews of global risk committee membership to ensure the right balance of functional, divisional, location and skill representation.

Source: <https://www.intertek.com/siteassets/investors/2024/intertek-annual-report-2024.pdf>

Figure 37

Fresnillo 2024 ARA, p. 137

14

Tailings dams

(overflow or collapse of tailings deposits)

Risk description

Ensuring the stability of our tailings storage facilities (TSFs) during their entire lifecycles is central to our operations. A failure, collapse or overtopping of any of our TSFs could result in fatalities, damage to the environment, regulatory violations, reputational damage and disruption to the quality of life of neighbouring communities as well as our operations.

Before constructing a dam, we conduct a series of studies to confirm the suitability of the area. These studies include geotechnical, geological, geophysical, hydrological, hydrogeological, and seismic analyses. Before construction begins, the Ministry of Environment and Natural Resources (SEMARNAT), through the Federal Office for Environmental Protection (PROFEPA), conducts several assessments.

Most of our operative facilities were designed and constructed under local and national controls and standards; following investigation, re-design, and construction process over the last 4 years they also comply with Fresnillo's new tailings policy and guidelines.

Our understanding of historic facilities' conditions is not as mature as that of the operative facilities but is a work in progress. As such, those facilities remain on care and maintenance status (non-operative).

Having permits, licences and certifications from the government to be able to operate TSFs is a risk due to the time involved in these procedures and the legal complications. Planning new TSFs with the necessary time and to international standards is also a risk, due to the limitations of the land around our mines and the costs and time involved in constructing them. If we don't manage these in a timely manner, we run the risk of disrupting the operation.

Factors contributing to risk

- The climate in recent years has become harsher in the regions where we operate, i.e. more severe and prolonged rainfall, more intense air that takes away the geomembrane liners, snowfall, and frost that complicates the operation, etc.

Controls, mitigating actions and outlook

1. The Global Industry Standard on Tailings Management (GISTM) was published in 2020 and is considered to be best practice. We understand the value and importance it brings to our industry, and we continually review and assess the impact of compliance. Taking GISTM into account, we have updated our risk assessment methods with a focus on more detailed risk identification, failure modes, and controls to avoid catastrophic failures.
2. We launched a new tailings policy in 2023, based on the industry's best practices, reinforcing our commitment to the safety and health of our workforce, communities, and the environment. Each year, internal audit and external auditors specialised in tailings dams such as Hawcroft Consulting and 'Knight Piésold Consulting' check our compliance with the policy.
3. Catastrophic failures of TSFs are unacceptable and their potential for failure is evaluated and addressed throughout the life of each facility. We manage our TSFs in a manner that allows the effectiveness of their design, operation, and closure to be monitored at the highest levels of the Company:
 - Our TSFs are constantly monitored, and all relevant information is provided to the authorities, regulating bodies, and the communities that could be affected.
 - We manage our TSFs using data, modelling, and construction and operating methods validated and recorded by qualified technical teams and reviewed by independent international experts, whose recommendations we implement to strengthen the control environment.
 - Risk management includes timely risk identification, control definition, and verification. Controls are based on the consequences of the potential failure of the tailing's facilities.

4. In 2024 we continued several initiatives to align our governance practices with current best practices:

- Updating the inventory of the TSFs and validating the data log.
- Reviewing findings of the Independent Tailings Review Panel (ITRP) and prioritising recommendations arising from inspections.



For more details see Tailings and Mineral Waste Management on pages 95-97

External sources of confidence

- Complying with Independent Tailings Review Panel (ITRP) annual review program. This panel is comprised by renowned international experts.
- Periodically we are inspected by the Independent Tailings Review Panel, who issue corrective and preventive recommendations to keep the tailings dams in good condition. In 2024, the Independent Tailings Review Panel visits were made to all Fresnillo plc tailings dams.

Link to strategy



Risk appetite

Low

Risk owner

- TSF's Department
- Safety & Environmental Department

Risk oversight

- HSECR Committee
- Executive Committee

Behaviour

Stable

Risk rating (relative position)

2024: Medium (14)

2023: Medium (14)

Source: <https://www.fresnilloplc.com/media/zqcbodxt/46566-fresnillo-ar24-web.pdf>

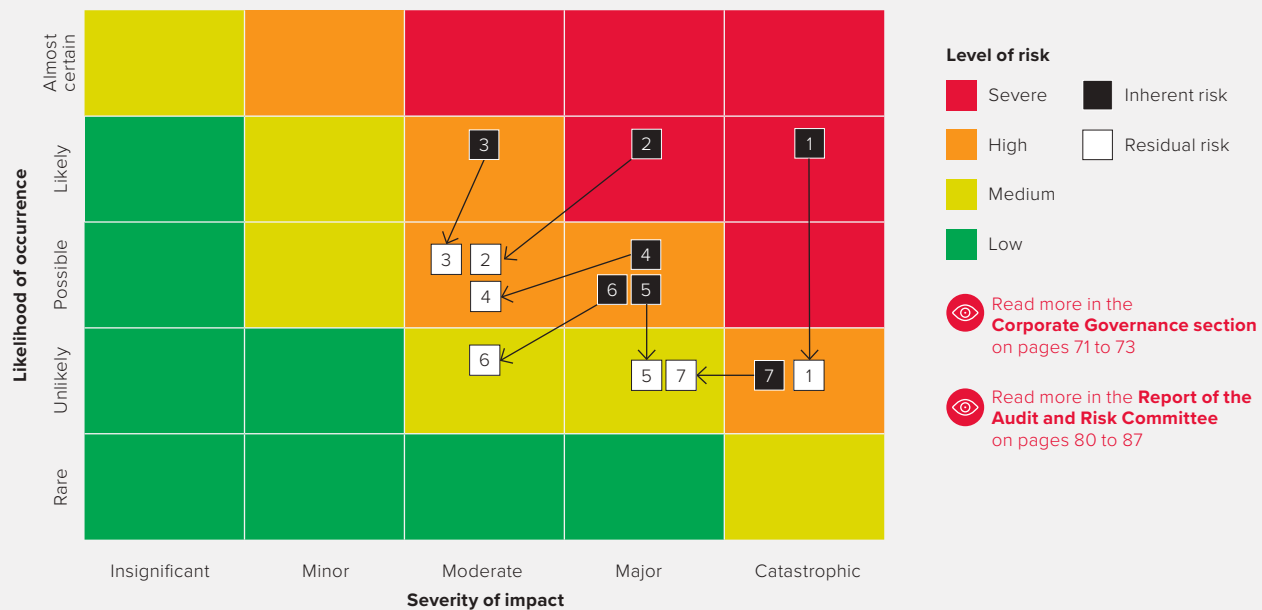
Figure 38

Mears 2024 ARA, p. 60, 86

Principal risk heat map

The Mears principal risk heat map as at 31 December 2024 is illustrated below:

The Group's risk register rates risks on a matrix scoring system based on their likelihood and impact, i.e. potential severity. This severity can be measured using life and limb, financial, customer service, growth, regulatory compliance and reputational criteria. Therefore, Mears measures more than simply the financial impact of the risk. These scores are used to escalate risks and to drive the mitigation plans.



No.	Risk title	Risk owner	Link to strategic pillar
1	Cyber attack including ransomware, phishing, hacking, data leakage or insider threat	Technology Director/Company Secretary	1 2 4
2	Breaches of health and safety and related legislation	Compliance Committee	1 2 3 4
3	Breaches of property standards and related legislation	Compliance Committee	1 2 3 4
4	Major data breach involving the release or publication of personal data	Technology Director/Company Secretary	1 2 4
5	Loss of AASC during contract period due to service failure, or failure to retain AASC or successor contractor at renewal	Chief Strategy Officer	1 3
6	Serious damage to brand following adverse event	Chief Executive Officer and Chief Strategy Officer	1 3 4
7	Large-scale Group-wide or nationwide incident such as pandemic, loss of IT systems or data, power cuts or communication system failures	Chief Executive Officer and Technology Director/Company Secretary	1 2

Effectiveness of internal control











































In relation to risk management and internal controls, the Board and Audit and Risk Committee are mindful of the importance of continuing to improve both control and output in this area. The co-sourcing between the internal Mears team and KPMG is believed to provide better and more focused audits, allowing KPMG or the Company to bring in specialists to complete a specific audit. We believe this to be a more effective and cost-effective approach when compared to employment of such specialists. The overall lead for our internal audit work continues to sit with KPMG, and there has been good continuity in personnel through the period. This was KPMG's third year under this co-sourced arrangement and saw the final year of the initial three-year plan. The work carried out during 2024, and the Committee's priorities for 2025, are detailed within this report.

As at the end of the period covered by this report, the Audit and Risk Committee, with the participation of the CEO and CFO, evaluated the effectiveness of the design and operation of disclosure controls and procedures designed to ensure that information required to be disclosed in financial reports is recorded, processed, summarised and reported within specified time periods.

We have conducted an annual review of the effectiveness of our risk management and internal control systems in accordance with the Code. Part of this review involves regular review of our financial, operational and compliance controls, following which we report back to the Board on our work and findings as described above. This allowed us to provide positive assurance to the Board to assist it in making the statements that our risk management and internal control systems are effective, as required by the Code.

The Company has in place internal control and risk management systems in relation to the Company's financial reporting process and the process for the preparation of the consolidated financial statements. The consolidated financial statements are supported by detailed working papers. The Audit and Risk Committee is responsible for overseeing and monitoring these processes, which are designed to ensure that the Company complies with relevant regulatory reporting and filing requirements.

Internal audit

Principal risk description		Inherent risk rating	Residual risk rating	Risk addressed in internal audit plan for the year			
				FY22	FY23	FY24	FY25
1	Cyber attack including ransomware, phishing, hacking, data leakage or insider threat						
2	Breaches of health and safety and related legislation						
3	Breaches of property standards and related legislation						
4	Major data breach involving the release or publication of personal data						
5	Loss of AASC during contract period due to service failure, or failure to retain AASC or successor contractor at renewal						
6	Serious damage to brand following adverse event						
7	Large-scale Group-wide or nationwide incident such as pandemic, loss of IT systems or data, power cuts or communication system failures						

Level of risk

 Severe  High  Medium

Source: https://cdn.prod.website-files.com/5ce1a07a0b5f0bd651245ae8/680f7b54be25fc92fb75a542_Mears-Group-PLC-Annual-Report-and-Accounts-2024.2.pdf

Figure 39

Helios 2024 ARA, p. 86

INTERNAL CONTROLS

At each Committee meeting we have a standing agenda item to review internal controls reporting, including the dashboard described below. We continue to mature the control environment, and the Committee discussed enhancements that are presented by management; for example in June, we reviewed the proposed monthly declaration for completion by OpCo senior management. We also consider annually our Financial Position and Projects Procedures (FPPP) procedures to ensure that this remains up to date in compliance with our continuing obligations.

CONTROLS DASHBOARD

The Group operates controls in key processes on a monthly basis. The focus of 2024 has been to review and where appropriate streamline controls ahead of key system changes in early 2025. Compliance control software is used to aid the preparation and monitoring of key reconciliations within the financial statement close process. These reconciliations are reviewed by management at both an OpCo and Group level. The Committee received regular updates regarding the development of the Group's new billing platform and the implementation of the new SAP platform, both of which will go live in early 2025, as part of our Finance Systems Roadmap. The Committee receives an update at each meeting regarding the control environment and operating effectiveness, including any follow-up actions or plans to enhance controls.

Example dashboard:

Process	December 2024									
	Group	East & West Africa			MENA		Central & Southern Africa			
	HoldCo	TZ	MW	SG	OM	DRC	GH	SA	CB	MD
P2P				1		1			1	
Fin reporting	2	2	2	2	2	2	2	2	2	2
Inventories										
Fixed Assets										
Revenue										
Taxation						3			3	
IT										

Key

- No control weaknesses
- Minor process improvements required
- Material process improvements required

Source: [helios-towers-2024-annual-report-interactive.pdf](#)

Figure 40

Admiral 2024 ARA, p. 143

Internal controls and risk management system

As in prior years, the Committee performed its annual assessment placing, in part, reliance on a third line of defence review of the Group's systems of internal control and risk management performed by the Internal Audit function. However, a slightly revised approach has been taken this financial year in preparation for the introduction of the updated UK Corporate Governance Code (2024), due to come into effect in 2025/26. During this financial year, the Group Head of Internal Controls and the Group Chief Risk Officer also presented an annual assessment of the Group's internal controls to support the Committee's own annual assessment.

In addition to the above assessments from management, and as in previous years, the Committee received a report from the Group Risk Committee on its activities to support the Group Audit Committee's annual assessment of the Group's system of internal controls and risk management. Further details of the Group Risk Committee's activities to support this process is outlined on page 148.

Both annual assessments provided by management, together with the Group Risk Committee's report on its supporting activities, provided the Committee with adequate assurance on the level and maturity of the Group's internal control environment and system of risk management, based on an overall improving position in relation to risk and controls across the Group.

Annual assessment key considerations:

- Internal Audit reports
- GRC reportable risk events (red and notifiable)
- Residual Risk - open GRC reportable risk events, open Category A and B internal audit recommendations
- Red Group KRIs with associated internal controls
- Whistleblowing events and coverage of training
- Group Compliance and/or Group Data Protection Privacy & Ethics Regulatory notifications
- Notable reputational events
- Group Minimum Standards (GMS) entity self-attestations
- Timeliness and completeness of Regulatory reporting
- Performance of key financial crime controls.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

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

© 2025 EYGM Limited.
All Rights Reserved.

EYSCORE 005805-25-UK
ED None

UKC-039952.indd (UK) 07/25.
Artwork by Creative UK.



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

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

ey.com