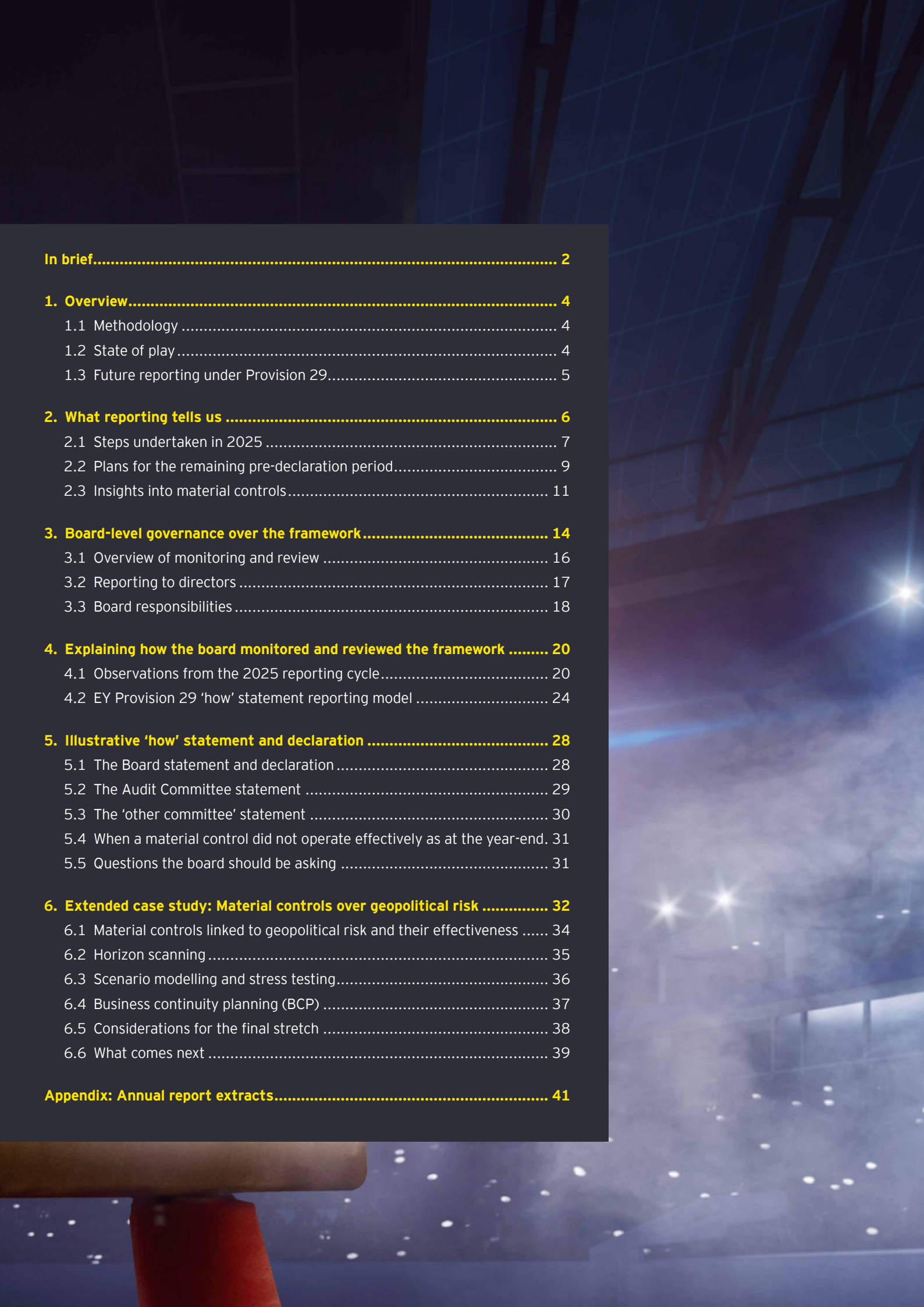
Provision 29: The final stretch

June 2026

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

Shape the future with confidence

Contents



In brief

Revised Provision 29 sets boards three tasks. They must monitor and review the effectiveness of the risk management and internal control framework, describe in the annual report how they did so, and declare whether material controls operated effectively as at the year-end. To see how boards are preparing for that first declaration, we analysed over 100 annual reports published in 2026 and continued our conversations with companies, building on our February 2026 paper, **The Goldilocks phase and beyond.**

Companies are well into the preparatory work, with emphasis shifting from design to execution. However, directors' own monitoring and review of the overall risk management and internal control framework (of which material controls are a part) has received far less attention both in the boardroom and in reporting. This, including clear distinction between the board's monitoring and review activities, needs to be an area of focus in the final stretch as it is the very thing that gives the declaration credibility. Boards will be best placed to make a defensible first-time declaration when they can demonstrate how monitoring, review and sources of confidence come together. To help boards with this aspect, including how to report on it clearly, Sections 4.2 and 5 of this publication set out our 'how' statement reporting model, an illustrative board statement and declaration.

In this final stretch, board agendas should include keeping information flowing clearly from management to the board and stepping back to ensure that previously identified material controls address the risks their businesses are facing today, given the volatility in the macro-economic and political environment. In this vein, we have included a case study in Section 6 which focuses on how material controls over geopolitical risk can be identified and their effectiveness assessed, as geopolitical risk was a principal risk for 61% of the FTSE 350 in the 2025 cycle.

Although we have titled this publication *The final stretch*, once the first declaration has been signed, further work will be required to turn the effort to date into proportionate, sustainable business-as-usual activity.

Authors

With special thanks to **Nidhi Arora**.

1. Overview

We are pleased to share *Provision 29: The final stretch*, the latest in our series of publications exploring the changes to the UK Corporate Governance Code. These require boards to explain how they have monitored and reviewed the effectiveness of the risk management and internal control framework (the 'how' statement), and to make an annual declaration on the effectiveness of its material controls (the 'declaration'). This is the final publication ahead of the first mandatory declarations, which will start to be published from mid-February 2027.

As companies enter this final stretch, the challenge will be to demonstrate that the board has exercised effective oversight over both the material controls and the framework as a whole.

In practice, this means being able to evidence how ongoing monitoring and the year-end review together support the board's conclusions. Where this is not well articulated, the credibility of the declaration may be undermined, regardless of the underlying work performed.

1.1 Methodology

To share insights promptly, findings in our February 2026 publication **The Goldilocks phase and beyond** were based on direct interactions with commercial listed companies across various industries and survey data.

The statistics presented in this publication are based on our review and analysis of 100+ FTSE 350 December 2025 annual reports. The observations are supplemented by analysis of an additional 25 annual reports of December 2025 small-cap companies and some FTSE 350 annual reports issued after April 2026, including a handful of non-December year-ends.

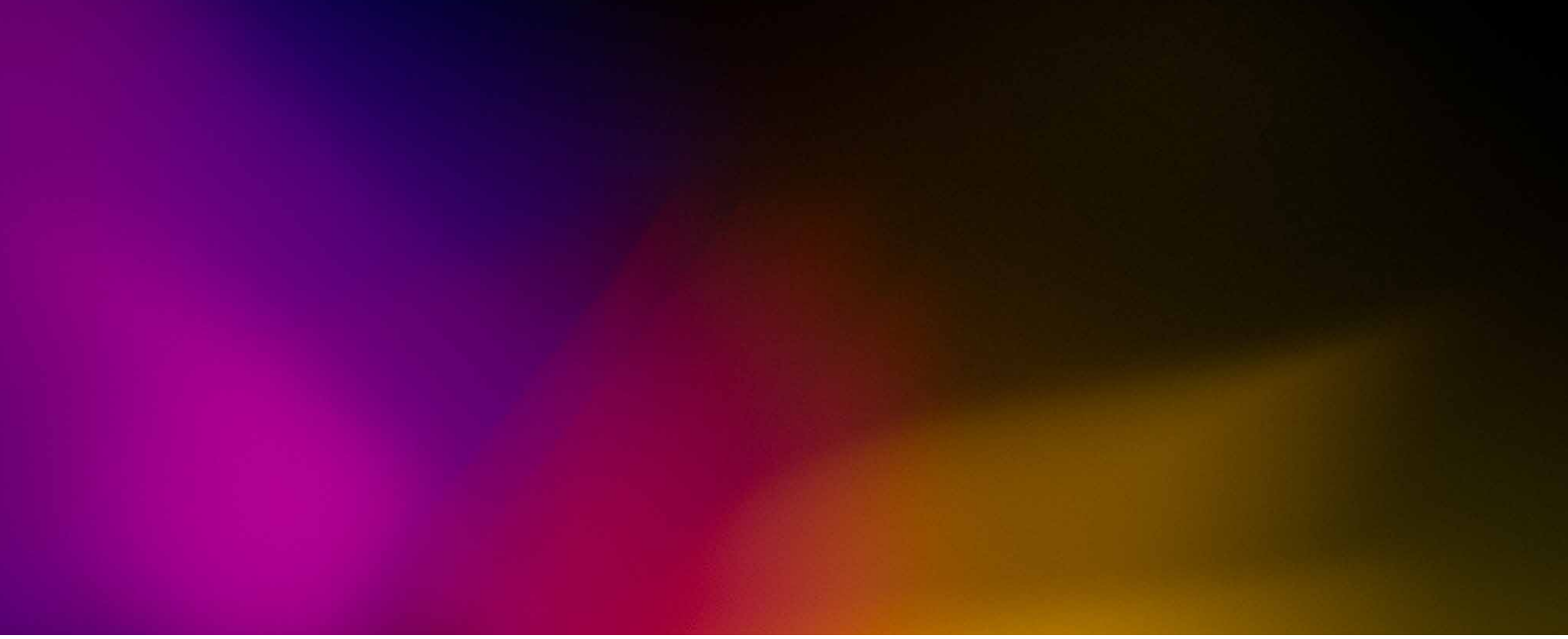
1.2 State of play

We summarise information gleaned from annual reports in **Section 2**. As there is no explicit requirement to disclose the activities undertaken to prepare for compliance with Provision 29, these disclosures should be interpreted in that context, and the absence of disclosure should not be read as the absence of activity.

What is evident from both disclosures and our discussions is that companies are at different stages of implementation, with some reporting activities that others had already completed in the prior year. This variation is similarly reflected in the areas of focus identified for the year ahead.

1.2.1 Final stretch

Regardless of relative progress, attention must now shift to determining precisely what information will be provided to the audit committee and, subsequently, to the board. The key challenges will be to agree not only its content (including the appropriate level of aggregation or granularity), but also its format – to enable directors to form, articulate and evidence robust, defensible judgements for their first declarations.



In the final stretch, companies will need to:

- Revalidate whether material control populations, criteria and confidence strategies remain appropriate.
- Consider whether any other refinements need to be made to the broader risk management and internal control framework to ensure that risk can be managed within risk appetite.
- Finalise communication pathways to the board.
- Review prior-year disclosures related to risk management and internal control, validate their accuracy and determine whether any enhancements are needed.
- Draft a preliminary 'how' statement and declaration.

1.2.2 Transitioning to business as usual

Companies will then face the task of transitioning their Provision 29 programmes and projects into a business-as-usual model, including:

- Enabling insights obtained from Provision 29-related activities to be regularly disseminated across the organisation.
- Embedding regular reassessments of design effectiveness of the framework and its material controls.
- Establishing sustainable approaches to assessing the operating effectiveness of material controls across the first and second line, and agreeing what level of internal audit involvement may still be required.
- Ensuring insights gained from Provision 29 projects inform committees' and the board's wider work, for example on internal audit use and oversight, crisis management and operational resilience.
- Adapting forward committee and board agendas and information flows to enhance the quality and consistency of monitoring undertaken by directors throughout the year.
- Ensuring the approach remains efficient and effective as the organisation, the risks it faces and the external environment evolve. This should involve assessing the need for, and the effectiveness of, operational and governance structures related to risk management and internal control, including those that have been established to date.

1.3 Future reporting under Provision 29

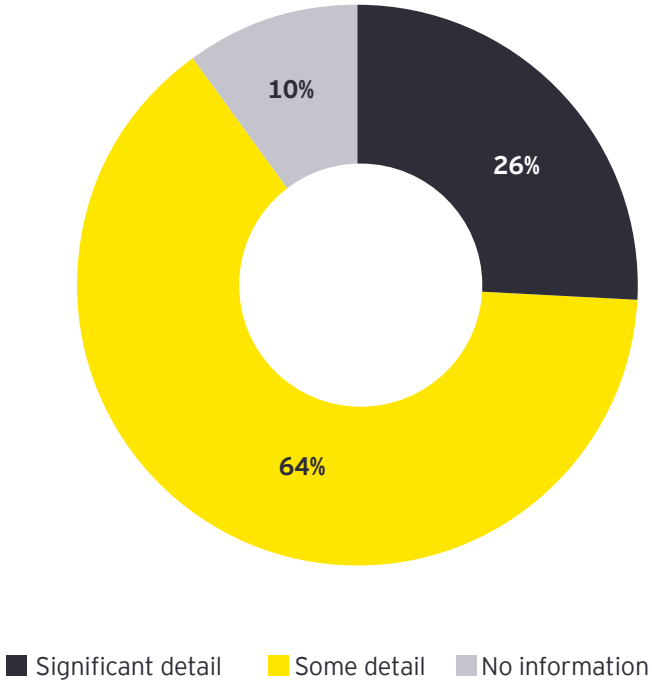
We have been asked by several companies to comment on draft 'how' statements and proposed material controls declarations. A common observation — consistent with our findings in **Addressing the new risk management and internal control requirements** — is that disclosures often blur two distinct sets of activity. The first is the monitoring that directors undertake throughout the year. The second is the additional work that supplements this monitoring to constitute the formal review of the framework, culminating in the material controls declaration.

We have therefore re-emphasised this distinction in **Section 3** of this publication and taken the opportunity to refresh our 'how' statement reporting model, as originally set out in **On track for Provision 29 compliance** in **Section 4**. To manage the size of this publication, we have not included the supporting extracts in the appendix, but a version of the model with reporting extracts drawn from the 2025 reporting cycle is available on request. **Section 5** includes an illustrative example of what the future reporting could look like. We hope it proves helpful as teams start putting pen to paper soon.

2. What reporting tells us

Most companies went beyond simply acknowledging that preparations for Provision 29 were underway: 64% gave some detail and 26% significant detail on steps already taken. By contrast, **very few** (17%) companies detailed areas of focus for the year ahead. In some cases, the disclosures did not clearly differentiate between what had already been achieved in 2025 and what was continuing into the year ahead.

Steps taken in 2025

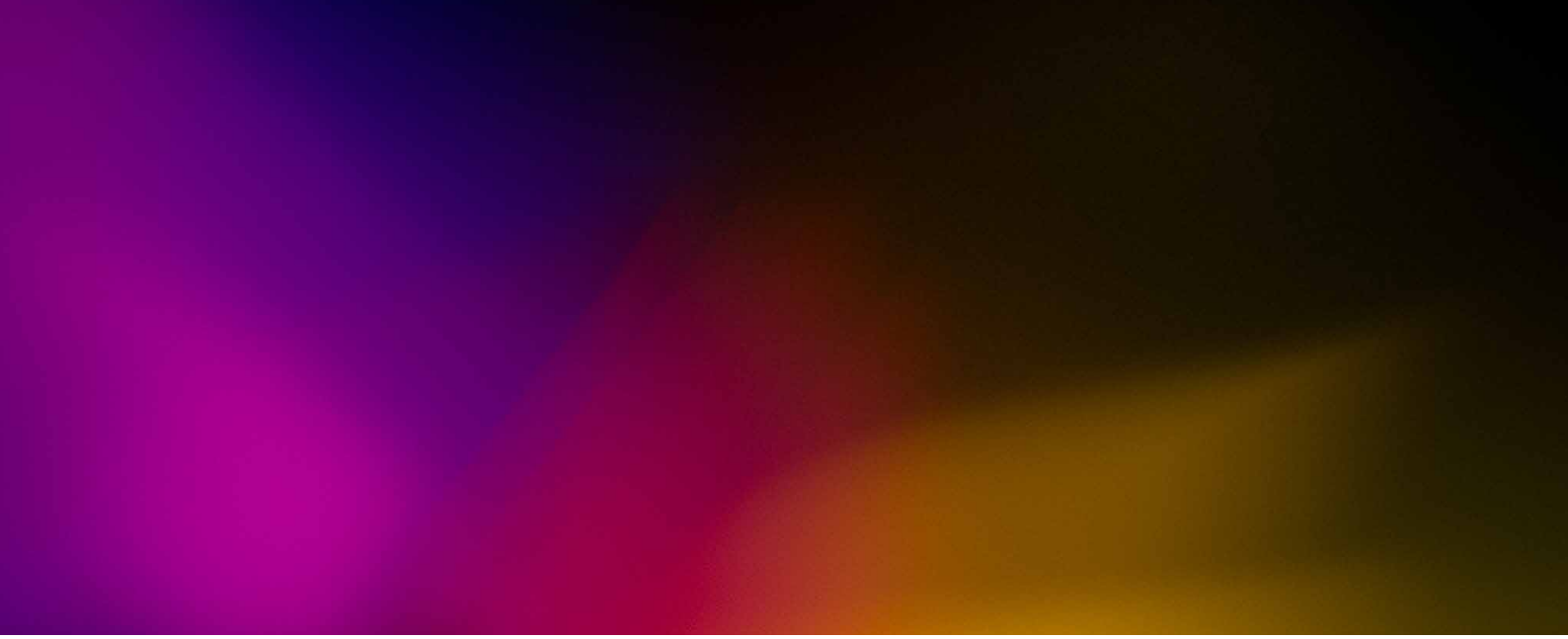


Activities such as identifying material controls, refining risk processes, strengthening governance and developing assurance evolve as understanding deepens. It was therefore not uncommon for the same focus area to be described as both having been undertaken and remaining a focus for the year ahead.

Establishing governance structures and updating terms of reference were more often described as having been completed. Similarly, review and challenge of underlying risks are now complete, forming the baseline for subsequent work. Activities relating to operating effectiveness testing, expanded assurance and declaration ready processes were more commonly framed as forward looking, even where initial steps have already been taken.

86% of companies we surveyed in early 2026 were planning or had already commenced dry-run activities; however, **only 29%** made explicit disclosures to this effect in their annual reports. Many others described activities typical of dry runs and pilots without explicitly referring to them as such.

Overall, the disclosures confirm what we noted in The Goldilocks phase and beyond, that preparation for Provision 29 is iterative rather than linear, with companies moving through overlapping stages as they transition from mobilisation and scoping towards developing confidence strategies and reporting approaches.



2.1 Steps undertaken in 2025

Activities discussed in our *On Track* publication as having been undertaken in 2024 continued to feature prominently in disclosures this year, reflecting differences in starting point, pace of progress and proportionality.

Companies largely focused on strengthening and clarifying existing risk management and internal control arrangements, rather than introducing new frameworks. This work centred on identifying and agreeing an initial population of material controls, developing approaches to building confidence over their effectiveness, and putting in place supporting governance arrangements. These steps were generally positioned as foundational, with many companies acknowledging that further refinement, testing and enhancement will follow in subsequent periods.

Only **a handful** (5%) of companies in our sample explicitly referenced third-party involvement in supporting their preparations. Where such involvement was described, it was typically positioned as providing challenge over the proposed approach. For example, Balfour Beatty noted that it appointed an independent third-party specialist to review Provision 29 readiness, with no significant concerns raised.

2.1.1 Risk management

In this area, disclosures note reviews of principal risks and deep-dive sessions with individual risk owners, as done by Melrose, alongside enhancements to the way risks are monitored and reported. For example, Energean (**Example 1**) refers to conducting risk pilots to (among other things) identify key risk indicators. Several companies also refer to updates to, or revalidation of, risk appetite, as noted by Trustpilot.

2.1.2 Material controls identification

A significant area of activity to date has been the initial scoping and identification of material controls, typically positioned as a preliminary or provisional step rather than a finalised position. Many companies describe having defined materiality criteria or thresholds for this purpose, as seen at Ocado (**Example 2**) and Hochschild. The audit committee of British Land emphasised the importance of a clear, proportionate and well-defined approach to materiality that appropriately reflected the scale and scope of the company's operations. In doing so, the committee was mindful of the need to avoid an overly narrow set of material controls, which could result in oversight being too high-level, and therefore supported an approach that enabled an appropriate depth of scrutiny. From our engagement, we know that some companies used risk scenario analysis as an input into material control identification and intend to use these scenarios to support borderline effectiveness judgements.

Companies also describe having identified an initial population of material controls, typically aligned with principal risks. Rotork, for example, refers to finalising its list of material controls in July 2025 (after a preliminary assessment in March 2025), while other companies describe this as an initial or provisional population, subject to further refinement.

Bunzl (**Example 3**) adopted a material controls policy and Tesco (**Example 4**) developed expected standards for its material controls to ensure they are designed to operate effectively.

Bunzl's new Material Controls Policy (Example 3), which covers financial, operational, reporting and compliance domains:

- Sets out the methodology for identifying and managing material controls (criteria, linkage to principal risks and disclosures).
- Aligns with the existing Risk Management Policy.
- Integrates the Internal Controls Essentials programme and similar functional frameworks to avoid duplication and to standardise evidence expectations.
- Clarifies accountability among management, risk owners and the committee for ongoing monitoring and the annual review of material controls.

Some companies also describe the implementation or enhancement of Governance, Risk and Compliance (GRC) tools to support documentation, monitoring and evidence retention, as noted by Wickes (Example 5). In some cases, companies clarify how material controls differ from 'key controls' previously documented within GRC tooling, as noted by Rightmove. Some, like ITV, also refer to clarifying ownership of material controls.

2.1.3 Approach to confidence

Alongside identification, companies have begun to consider how confidence over the effectiveness of material controls will be obtained. Activities described include mapping existing sources of confidence and updating assurance maps to identify gaps, as well as agreeing a proposed approach to building confidence over time.

Around a quarter (24%) provided good insights into the sources of confidence specifically over material controls, with many others discussing this in respect of the framework more broadly. In some cases, it was difficult to discern whether particular activities related to material controls or underlying key controls. Disclosures confirm what we noted in The Goldilocks phase and beyond, that companies are developing confidence through a layered approach, beginning with first-line attestations, reinforced by second-line activity, and supported by internal audit assurance, with external assurance or specialist input used more selectively.

Although not always explicitly linking this to Provision 29 preparations:

- **15%** of companies refer to assurance mapping.
- **65%** discuss enhancing or introducing testing of internal controls (not just material controls).

First-line activities

Companies most commonly describe first-line activities as the starting point for building confidence over the effectiveness of material controls. These are typically framed as structured management level attestations, often done quarterly, providing direct confirmation from those responsible for operating the controls. For example, Informa refers to quarterly self-certfication of control effectiveness, Breedon (Example 6) references annual attestation of effectiveness from each process owner and Wickes (Example 5) notes that control owners and performers started to record the performance of their controls and perform regular self-assessments.

Second-line activities

Some companies also describe second-line activities as a source of confidence, where specialist functions undertake active testing or challenge of control operation. For example, Intertek refers to assurance activity performed by the compliance function over non financial and operational controls and by the cyber security functions over IT controls, while Tesco (Example 4) notes that second-line functions, such as finance controls, ethics and compliance, and safety, systematically test key processes and controls as part of the overall confidence framework. Trustpilot discloses that it engaged external support to review its approach, carry out testing of design and operating effectiveness and make recommendations to strengthen the coverage and effectiveness of its material controls framework.

In fact, based on our engagements with companies, we understand that building out second-line capabilities is one of the most visible consequences of Provision 29 implementation outside of financial services.

41% of companies referenced testing material controls, with no FTSE 350 companies in our sample referencing external third-party involvement in material controls testing.

Rio Tinto explicitly stated that no external assurance had been sought over material controls.

Third-line activities and external sources of confidence

Internal audit involvement was frequently cited as part of the confidence landscape. Activity included testing the design and effectiveness of material controls and plans for retesting following remediation. It was not uncommon for companies to note that these activities were selective, risk based or rotational. For example, Pearson (Example 8) and Genuit refer to a model involving cyclical or rotational testing of controls. THG notes that it had entered into a formal internal audit co-source to maintain an adequate level of assurance across its 'Cyber security and data privacy' principal risk, among others.

References to external independent assurance or specialist input are less prevalent and, at this stage, have not been linked directly to confidence over material controls. For example, Trustpilot refers to a Service Organization Controls (SOC) 2 Type 2 attestation, and Gamma lists out its ISO certifications.[1] These will clearly contribute to the overall confidence in the effectiveness of the risk management and internal control framework, but how these contribute to evidence material control effectiveness is not explicit. Most common were references to external sources of confidence regarding cyber risk, often in the context of National Institute of Standards and Technology (NIST) cybersecurity maturity assessments conducted by external providers. In fact, **28%** of companies that have implemented the NIST Cybersecurity Framework tend to obtain some form of external validation, albeit the disclosures are not always clear as to whether this was undertaken in the given year.

Serco noted that an external quality assessment of its Enterprise Risk Management function had been undertaken in 2025 and that the suggestions identified for continuous improvement will be reviewed for implementation in 2026.

2.1.4 FTSE small-cap observations

A recurring and explicit theme across the small sample of FTSE small-caps was the emphasis on documentation and consistency. Companies typically framed their Provision 29 preparation in terms of documenting key business processes and material controls, refreshing or standardising control frameworks, and establishing a more consistent group-wide approach to identifying, describing and evidencing controls. Language such as 'consistent and transparent format', 'consistent group-wide approach', 'robust documentation', 'formalisation and standardisation' and 'developing a consistent methodology' appeared repeatedly across disclosures. For example, Capita stated that during the year its Audit and Risk Committee oversaw delivery of the next phase of its Internal Control Framework programme, aimed at strengthening the Group's underlying control environment and building a more consistent, group-wide approach to documenting, assessing and assuring material controls.

Compared with the FTSE 350, a greater proportion of small-cap companies appeared to be at earlier stages of their compliance journey. Several disclosures focused on refining principal risks, strengthening second-line capabilities, or preparing for the identification of material controls, with some noting that an initial list of material controls had not yet been agreed. These patterns mirror those observed in the EY 2025 FTSE 350 On Track analysis.

Around three-quarters of the small-cap companies reviewed explicitly referenced internal audit involvement in their preparations for Provision 29, most commonly in relation to assurance planning, alignment of audit plans to material controls, or future testing and validation activity. One company, Synthomer, described appointing a third-party expert to help identify, review and test its material controls.

2.2 Plans for the remaining pre-declaration period

Forward looking disclosures indicate that companies are planning to build on earlier preparatory work as they move closer to their first Provision 29 declaration, with a particular focus on material controls refinement, testing, effectiveness assessment and governance reporting. Howden Joinery (Example 9) confirmed that its Audit Committee *'anticipates that it will report in full against Provision 29 in the 2026 Annual Report and Accounts'*.

2.2.1 Refining the population of material controls

Disclosures indicate that companies are planning to continue and complete earlier identification work, rather than shift focus entirely. A recurring theme is the refinement of the population of material controls, including extending and revalidating initial identification activity.

This is explicitly described by companies such as Molten Ventures (Example 10), Harworth and Melrose, which note that further refinement, expansion or validation of material controls is planned as preparation continues.

1. A SOC 2 Type 2 report is an independent assurance report verifying that an organisation's internal controls regarding data security, privacy and system availability are not only designed correctly but effectively operating over a sustained period (typically 6 to 12 months).

2.2.2 Refining approaches to control effectiveness

Annual report disclosures also provide clear examples of companies refining their approaches to assessing control effectiveness, alongside the expansion of assurance activity. Melrose states that, looking ahead to 2026, senior management is developing an 'assurance and testing matrix' to articulate how assurance over each material control is built to 'evidence the effectiveness of each material control', with the intention that this will form the base framework for future assurance cycles. Rightmove notes that discussions will continue during 2026 on 'how to measure control effectiveness', among other things, alongside refinement of the draft list of material controls.

2.2.3 Expanding testing and other confidence activities

An area that does not feature explicitly, but that from conversations we know is taking place, is the expansion of testing and other confidence activities. While some companies refer to initial design effectiveness testing or pilot activity, plans to increase the coverage and depth of testing in the coming year can be inferred from some disclosures. For example, Drax describes plans to enhance second-line assurance underpinning IT controls and C&C Group notes that it commenced a testing programme for material controls in FY26 with further plans in FY27. Harworth notes that its key risk indicators (KRIs) used to measure the profile of each risk remain under development, and that its ERM function aims to improve their quantity and quality, and to develop a KRI dashboard for continuous real-time monitoring of KRIs where possible. Risk reporting will be embedded into operational dashboards as a 2026 priority to provide real-time visibility, enabling faster, better informed decision-making.

2.2.4 Summarising findings

With multiple sources of confidence and many ongoing activities, companies are developing consistently structured outcome summaries to support the conclusion process. As discussed in The Goldilocks phase and beyond, many do this at the principal risk level, while others adopt a material controls approach, although the content remains broadly similar. Contributing data points include risk and control self-assessments, KRIs, incident reports and internal audit input. These summaries are provided to the material control owner, who, alongside engagement with the principal risk owner and their own knowledge of the business, concludes on effectiveness and documents the rationale, including any departure from a purely formulaic interpretation of the data. Information provided to the audit committee and subsequently to the board should be a natural follow on from the above, carefully calibrated for depth and granularity appropriate for non-executive directors. United Utilities (**Example 11**) developed a material controls reporting tracker summarising the material impact risks and associated material controls, a view and explanation of the effectiveness of the controls and any supporting assurance.

It is increasingly clear that binary approaches do not work in practice; even traditional three-tier RAG ratings are proving insufficient, with companies moving towards more graduated outcome categories such as effective/mature, room for improvement, needs improvement and unsatisfactory.

Companies continue to debate how to translate weaknesses in underlying key controls into effectiveness considerations of the related cluster and single-risk framework material controls. As noted in The Goldilocks phase and beyond, issues in the effectiveness of underlying key controls do not automatically equate to material control ineffectiveness, as long as they are being picked up and promptly remediated. It is worth clarifying however that if these problems continue to be numerous or very serious, this might indicate that other elements of the material control, like policies and related training, require attention.

2.2.5 FTSE small-cap observations

Consistent with the FTSE 350 experience, small-cap companies also commonly referred to assurance maps, plans for testing material controls, and dry runs or pilot exercises, most of which were positioned as activities planned for the rest of 2026 rather than completed in 2025. Disclosures also point to a focus on operationalising assurance maps, embedding periodic review and reporting arrangements, and using the outcomes of testing to remediate weaknesses and further strengthen documentation. For many small-caps, the remainder of 2026 is therefore likely to be intense. They will need to develop, refine and finalise their control and assurance frameworks, identify their material controls, and assess both design effectiveness (with some dry runs not happening until the third quarter) and operating effectiveness. In this vein, Mears (**Example 12**) clearly sets out the planned activities over the remainder of 2026.

2.3 Insights into material controls

The survey data quoted in **The Goldilocks phase and beyond** indicated that more than 80% of companies had already identified material controls. Yet only around a third (33%) provided a material controls definition, disclosed the criteria applied in identifying material controls (as Ocado did), or confirmed that a definition had been agreed.

2.3.1 Material control definitions

Disclosures typically indicated that material controls are linked to the principal risks and additionally cover IT general controls and financial and non-financial reporting. Some stated that material controls are those that are most critical to long-term sustainability or most critical to mitigating risks that could adversely affect long-term success. Some companies noted that their definition was informed by factors such as financial impact, regulatory or legal consequences, stakeholder impact, strategic importance and public interest considerations.

> “
>
> The Group has defined material controls as being those controls over which the Board considers external stakeholders would want to receive assurance about their adequacy and effectiveness, and we have identified c.30 controls that meet this criteria.
>
> Eurocell 2025 annual report

> “
>
> The material controls are designed to manage each inherent principal risk down to an acceptable level of residual risk which is within tolerance of our stated risk appetite, rather than aiming to eliminate the risk altogether. This approach allows us to recognise that conscious risk management can also include potential benefits and enables us to make informed decisions, enabling the business to grow safely whilst delivering good client outcomes.
>
> Material controls are critical to managing the principal risks that could threaten the business model, future performance, solvency, liquidity and reputation, or affect the long-term sustainability and resilience of the business. The scope covers all material controls including financial, operational, reporting and compliance.
>
> JTC 2025 annual report

2.3.2 Linking material controls to principal risks

A number of companies noted which risk areas had material controls identified against them, with Persimmon doing this explicitly as part of the principal risk disclosure. BT (Example 13) explains that it divides its risk landscape into 13 Group Risk Categories (GRCs). Each GRC has an Executive Committee sponsor accountable for applying the risk management framework to that category. Each GRC framework includes the five elements: governance and oversight; risk appetite; dynamic risk management; policies, standards and controls; and Assurance. Each GRC framework has been defined as a material control. BT supplements these GRC frameworks with company-wide material controls that include the code of conduct and training, the speak up process, the disclosure committee and the delegation of authority framework.

United Utilities (Example 11) defines material impact risks as those of its principal risks, which, in a remote but plausible scenario, could initiate corporate failure. The future material controls declaration will be in respect of the key controls which mitigate material impact risks. These have been listed alongside the material impact risks, together with governance and assurance.

> “
>
> Following analysis of risk scenarios, the Audit Committee has established a subset of risks and controls to be classed as material for ongoing monitoring and reporting to the Board. These material controls represent the critical judgements and higher-level elements of the controls environment underpinning the Group’s material operational, compliance and reporting risks.
>
> Burberry FY26 annual report

2.3.3 Examples of material controls

Beyond the three companies mentioned above, only a limited number provide concrete examples of material controls.

Breedon (Example 6) gives delegation of authority and whistleblowing as examples of entity-level material controls. SThree states that horizon scanning remains a material control. Spire Healthcare lists out key financial reporting controls within its material control framework, which include budgeting and monitoring, forecasting, capital expenditure authorisation, segregation of duties and balance sheet reconciliations. A few, such as Inchcape (Example 7), specifically reference cyber controls without setting out what these are. Bunzl (Example 3), on the other hand, describes its cybersecurity risk mitigation framework, although does not explicitly label this as a material control. Similarly, JD Sports Fashion references the development and imminent launch of a Technology Risk and Controls Management Framework.

Hunting (Example 14) provides a combination of material control examples and areas. JTC (Example 15) provides a list of material controls and mitigation measures — without differentiating between the two categories. Molten Ventures (Example 10) discusses its 40 material controls organised into four primary categories, aligned with the UK Corporate Governance Code. Aston Martin describes recognising 21 material control areas including financial reporting and disclosure; IT general controls and cyber security; data governance and data quality; conduct, regulations and compliance; supply chain and third-party risk; treasury, liquidity and capital management; business continuity and operational resilience; and ESG reporting, including climate related disclosures.

2.3.4 Expectations going forward

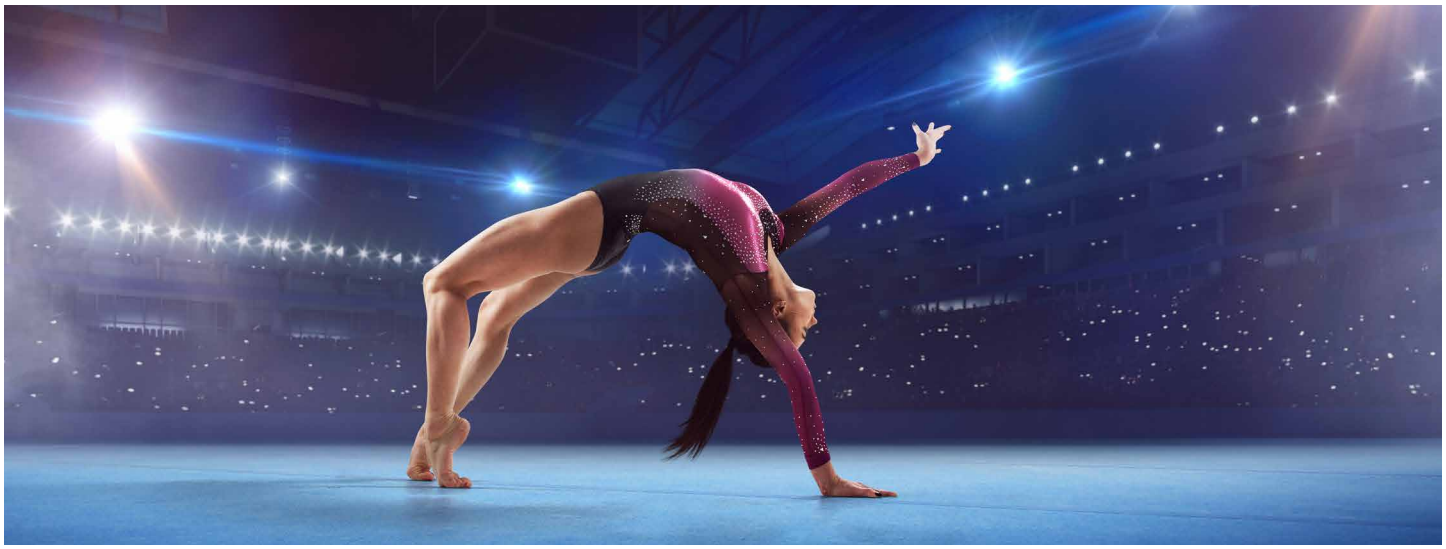
Given that there is no requirement to describe material controls unless they did not operate effectively as at the balance sheet date, we expect that the number of companies providing detailed examples will remain low. Even where disclosure of a material control becomes necessary, we anticipate that companies are likely to address this by reference to the risk area the control was intended to address, rather than providing a detailed control level description. This reflects the idiosyncratic nature of material controls, which often do not lend themselves to concise, standardised explanations that are readily understood by external users.

However, describing how material controls are identified, differentiated from broader risk responses, or positioned within the wider internal control and risk management framework, as done by Tesco (Example 4) in respect of internal controls over financial reporting (ICFR), provides valuable clarity. It helps users assess the robustness and consistency of approaches across the market. We therefore encourage companies to consider providing such disclosures on a voluntary basis. As some companies also mention testing key or underlying controls, being explicit about what these are in the context of material controls is also likely to be helpful to readers.

Our point of view

While it is for boards to determine what constitutes a material control, in our view it is important to avoid conflating the following:

- **Material controls with sources of confidence over the risk management and internal control framework.** For example, external audit can be a source of confidence to the board, but it is not itself a material control over financial reporting.
- **Non-executive directors' governance responsibilities with the execution of material controls.** For example, board approval of a strategic acquisition is an important governance activity, but it is not a material control addressing the risk of entering into a disadvantageous transaction.

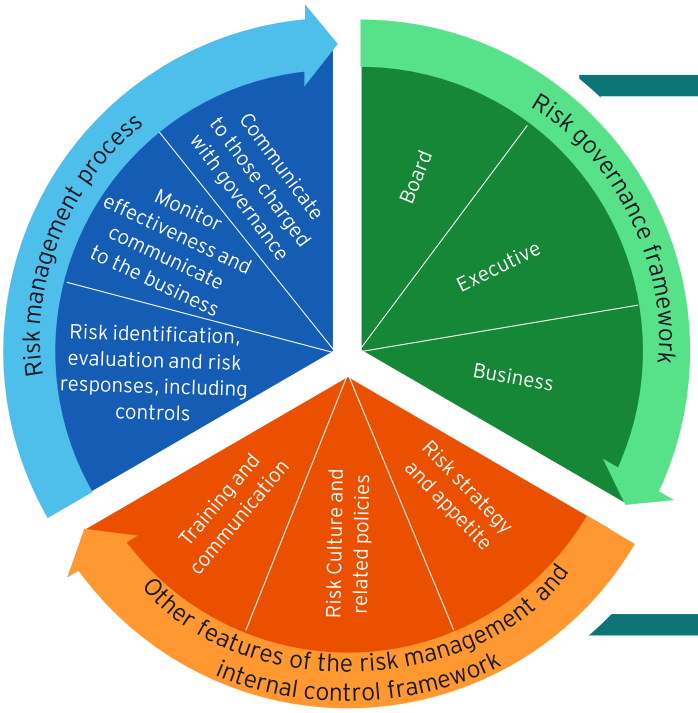


3. Board-level governance over the framework

Amendments to Provision 29 have clearly acted as a catalyst for strengthening risk management and internal control frameworks. In practice, however, dry-run activity has tended to focus on executing the agreed confidence strategy for material controls and has often involved testing underlying key controls. In most cases, the primary objective was to identify and remediate gaps in effectiveness.

Boards should remember that Principle O now requires the board not just to establish but also to maintain an effective risk management and internal control framework. Provision 29 requires them to monitor and review the effectiveness of the risk management and internal control framework as a whole (and describe how this was done), not solely to reach a conclusion on the effectiveness of its material controls.

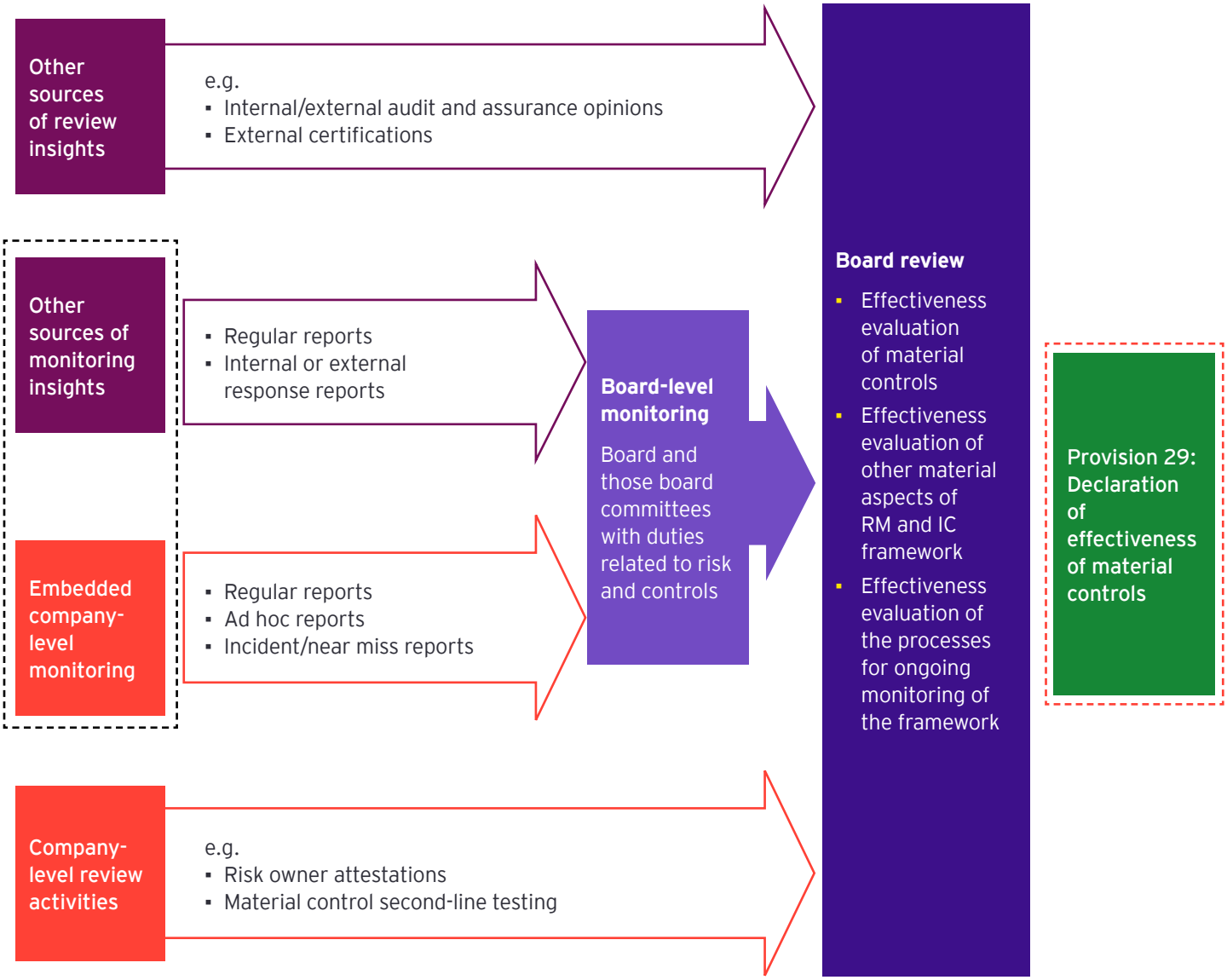
Guidance 293: Describe the main features of the framework (...)



- Internal Audit
- External Audit
- External Board reviewer
- ISO certifiers
- Other assurance providers
- Other subject matter experts

- 1st line
- 2nd line
- Business Unit/ Division
- Executive

Provision 29: Describe how the board monitored and reviewed the risk management and internal controls (RM and IC) framework



3.1 Overview of monitoring and review

Both monitoring and review serve to identify and evaluate areas for improvement in the design, operation and maintenance of the risk management and internal control framework. However, the former is an ongoing process aimed at identifying issues in a timely way so they can be promptly addressed, and the latter leads to a point-in-time conclusion on effectiveness, including on the effectiveness of material controls.

Directors should differentiate between those activities that might be spread across the year but provide views on effectiveness at a point in time (such as outcomes of multiple internal audits or risk deep dives) and those activities that allow for ongoing monitoring of the framework, such as analysing KRI reporting.

The FRC guidance considers company-level monitoring, board-level monitoring and board-level review of the risk management and internal control framework to be three separate concepts:

Company-level monitoring

261 The company should have systems in place to carry out ongoing monitoring of the design, implementation and operation of the risk management and internal control framework. (...)

Board-level monitoring

263 The board cannot rely solely on the embedded monitoring processes within the company to discharge its responsibilities. It should conduct its own monitoring, based on the regular reporting and other communication with management, internal audit, external audit and other appropriate functions and units. (...)

Board review

278 There is no single way of carrying out a review. The board may wish to define the processes to be adopted, including drawing on the results of the board's ongoing process such that it will obtain sound, appropriately documented, evidence to support its reporting in the company's annual report and accounts. It should ensure that it has considered all material aspects of the framework.

In alignment with this, SSE notes that its board, supported by the audit committee, oversees and challenges management's approach through its own monitoring and review of the integrated assurance activities, to support the board's annual report effectiveness declaration.

Board-level monitoring relies on outputs of embedded company-level monitoring supplemented with additional sources of insights. These will be a combination of:

- **Regular reports,** the formality, scope and frequency of which directors will need to agree.
- **Ad hoc reports,** including incident reporting and near misses – directors should agree data points or event types (e.g. regulatory breaches or fines) that would trigger the need for ad hoc communication.
- **Response reports,** commissioned by directors to address a particular issue.

Provision 2 of the Code requires the board to assess and monitor culture and how the desired culture has been embedded, and to explain the board's activities and any action taken. Reporting on how the board monitored culture, using reports from management, other sources of insights and its own engagement under Provision 5 of the Code, has evolved significantly in recent years. Disclosures like those of Metro Bank (Example 16) can be used as inspiration for enhancing risk management and internal control reporting.

To address timing lags, conclude on remediation activities, and form a view on those aspects of the framework that operate primarily around the year-end, the board's review will need to draw on the outcomes of prior board-level monitoring and be supplemented with targeted review specific insights, such as:

- Internal/external audit outcomes and observations.
- External certifications and assurance opinions.
- Risk owner self-attestations, year-end risk dashboards and follow-up on risk deep-dives conducted earlier in the year.
- 'No change' confirmations related to other areas covered earlier in the year.

- Material control year-end effectiveness assessment, which can include owner self-attestations, second-line reviews or independent testing.
- Confirmations that remediation activities have been completed.

The FRC guidance advocates particular focus on previously reported issues and weaknesses in the operation of material controls and actions being taken to address them.

3.2 Reporting to directors

Although much more limited than those relating to material controls and their effectiveness, some disclosures did refer to improving the quality and cadence of information provided to directors, updating terms of reference and governance processes, as noted by Ocado (**Example 2**), and rolling out communication and training to risk owners and control owners.

In addition, several companies describe specific plans to enhance the quality of board level reporting in relation to material controls and their effectiveness. Harworth highlights plans to streamline risk reporting by embedding it into operational dashboards for real-time visibility, while Rotork refers to the development of a proposed annual assurance reporting framework from 2026 onwards to support assessment of material control effectiveness.

Both from disclosures and from conversations, not many companies used their dry runs to trial updates to ongoing monitoring activities. In most cases, dry-run activity stopped short of piloting what year-end reporting to the board for the formal review would look like. References to mock declarations were not common, although we know from our engagement that many companies were planning for this post year-end.

Some exceptions include:

- Tesco (**Example 4**), which developed a robust end-to-end sign-off process with material control owners and simulated the roll-up for the board declaration process.
- Marshalls, which undertook a pilot to refine controls and outputs of the assurance process, culminating in a mock declaration to agree anticipated wording for 2026.
- Energean (**Example 1**), which developed a Key Controls Repository, and Risk-Pilot sessions, to support clearer, more structured information being provided to the board.
- Just Group, which enhanced documentation and evidence to support future board attestations and developed reporting templates and governance processes for annual review and sign-off.
- United Utilities (**Example 11**), whose audit committee emphasised the importance of the board having early sight of and fully understanding what information would be presented to it in order to make the declaration.

To truly build on progress to date, additional effort will be needed to establish a more robust business-as-usual director-reporting framework that is sustainable. Disclosures indicate that, in the run-up to the first declaration, the level of detail being presented to some audit committees may have been excessive, mirroring information presented to the executive.

Hunting (**Example 17**) stood up an Internal Controls Committee that works with the Executive Committee and reports directly to the Audit and Risk Committee. Where companies had set up similar executive-level steering committees to implement the Provision 29 changes, decisions will need to be made as to whether these new structures will remain as part of business as usual.

3.3 Board responsibilities

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

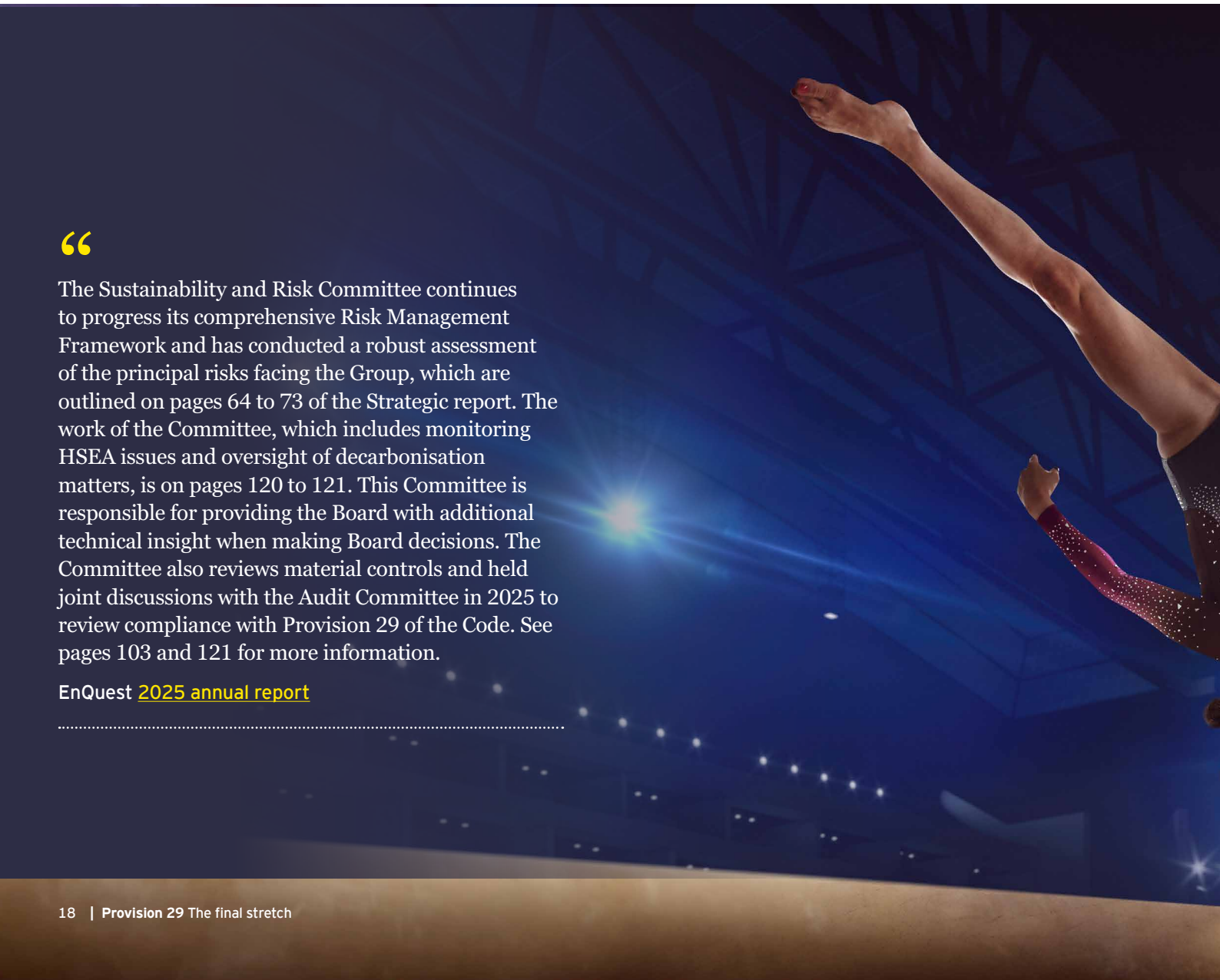
3.3.1 Committees with risk-related responsibilities

Although **41%** of companies in our sample have board level committees beyond the audit and/or risk committee with explicit risk oversight responsibilities (very often ESG or sustainability committees), only a small number – including Glencore, Spire Healthcare and Pearson – explicitly confirm their involvement in supporting the board's material controls declaration. THG reassessed how information is captured and presented to the relevant committees, to support the disclosures the board will ultimately need to make.

Of the **27%** of companies in our sample with a risk committee, **43%** were explicit about cooperation between the audit committee and the risk committee in relation to Provision 29, as disclosed by Standard Chartered (**Example 18**). In some other cases, such cooperation could be inferred from broader statements referring to oversight of the overall risk management and internal control framework, for example: 'The Board, supported by the Audit Committee and by the Risk Committee, monitored the effectiveness of the Group's risk management and internal control framework throughout the year.'

3.3.2 Aggregating at the board level

Regardless of how responsibilities are allocated, the board ultimately acts as the overall aggregator, and the declaration on the effectiveness of material controls will be approved by the unitary board. Directors therefore need to agree how information will flow from board committees – most notably the audit (and, where relevant, risk) committee – up to the board.



"

The Sustainability and Risk Committee continues to progress its comprehensive Risk Management Framework and has conducted a robust assessment of the principal risks facing the Group, which are outlined on pages 64 to 73 of the Strategic report. The work of the Committee, which includes monitoring HSEA issues and oversight of decarbonisation matters, is on pages 120 to 121. This Committee is responsible for providing the Board with additional technical insight when making Board decisions. The Committee also reviews material controls and held joint discussions with the Audit Committee in 2025 to review compliance with Provision 29 of the Code. See pages 103 and 121 for more information.

EnQuest 2025 annual report

Our engagement to date suggests that this final aggregation step has not yet been fully worked through in many cases. How it operates in practice will depend on the board's governance model and the way its committees function:

- Where boards already place significant reliance on the audit committee, this is expected to continue for the purposes of the declaration, with boards relying primarily on the audit committee chair's reporting rather than reviewing additional information on material controls at board level.
- In other cases, companies have indicated that the board will receive a report summarising the information provided to the audit committee as part of its review.

We also understand that decisions on the level of detail presented to the board will depend partly on whether directors who are not on the audit committee typically attend its meetings, and so already have visibility of the underlying discussions.

Where the audit committee is required to exercise significant judgement, for example, if an agreed effectiveness criterion has not been met, in our view it would be appropriate for the committee to inform the board of that judgement and explicitly seek its input. This enables the board to understand the basis for the conclusion, apply appropriate challenge, and satisfy itself that the judgement reached provides a sound and defensible foundation for the declaration.

From our engagement with companies, questions about the appropriate reference point for forming judgements on material control effectiveness continue to arise. In our view, a key consideration is whether the related risk has been managed within the organisation's risk appetite.

4. Explaining how the board monitored and reviewed the framework

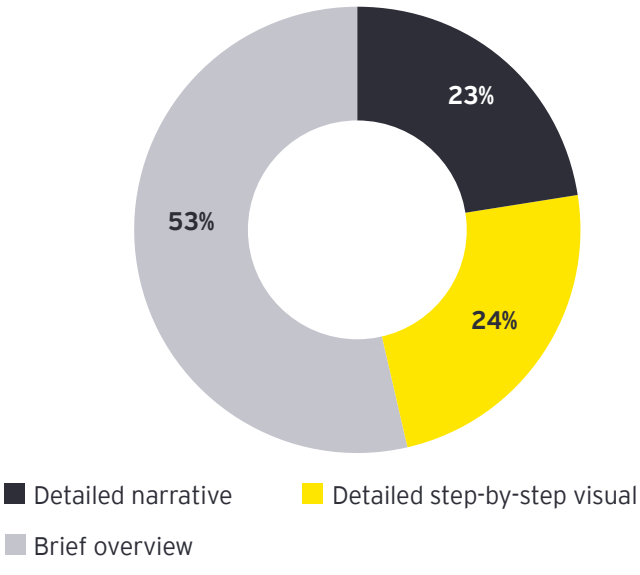
There is no standard or framework underpinning the duties and requirements embedded in Provision 29. A full narrative explaining what enabled directors to reach a conclusion on material control effectiveness and make the declaration is therefore important. It gives readers of the annual report confidence in the declaration's veracity. Companies will need to strike the right balance in their disclosures between credibility and over-disclosure.

4.1 Observations from the 2025 reporting cycle

4.1.1 Main features of the framework

Our analysis of ARAs indicates that most companies follow the FRC's Guidance 293 recommendation and describe the main features of their risk management and internal control framework. Some **88%** of companies describe their risk governance framework in the risk management section, and all companies discuss the risk management process, albeit to a different degree of detail.

Risk management process disclosures



The approach to describing other features of the framework in the risk management section is less consistent. While 43% of companies reference the approach to setting risk appetite, elements such as training and communication might be discussed elsewhere in the annual report, but few companies cross-refer to them as part of this narrative.

Furthermore, while disclosure of board oversight of culture has become relatively well developed, outside the financial services sector there is limited reference to how the desired risk culture is embedded. Where culture is discussed, the narrative tends to focus on diversity and inclusion rather than on risk behaviours and conduct. Airtel Africa (Example 19) includes 'promoting, assessing and embedding risk and ethical culture across the organisation' as one of its audit committee's risk management priority areas.

The Spotlight on monitoring and reviewing culture included on pages 22-23, may provide companies with practical tips.

Some **88%** of companies describe their risk governance framework in the risk management section.

4.1.2 Board-level monitoring and review

There was an increase in the number of companies that concisely articulated what directors considered as part of their monitoring and review activities, and how this informed their conclusions, including disclosures by Rolls-Royce (**Example 20**) and Bunzl (**Example 21**).

However, the narrative continued to focus primarily on the risk management process element of the framework, emphasising management and internal audit activities more than how directors used their outputs and the outcomes that resulted.

Narrative relating to other aspects of the risk management and internal control framework remained limited. For example, assessing the appropriateness of risk management structures at both board and executive level may from time to time form part of an effectiveness review. In practice, however, such considerations were seldom linked explicitly to the broader Provision 29 disclosure.

Furthermore, in many cases it remained difficult to distinguish clearly between activities that constituted ongoing monitoring and those that formed part of the review. As noted in **Section 3.1**, this distinction is important in ensuring that the board's conclusion on effectiveness is supported by appropriately documented evidence. Ongoing monitoring provides insight into trends, issues and remediation over time, while the review draws these strands together to support a point in time assessment and a robust and defensible declaration. Treating monitoring and review as separate but connected activities strengthens both governance discipline and reporting clarity.

Spotlight on monitoring and reviewing risk culture

A key component of the risk management and internal control framework is risk culture – the behaviours, attitudes and incentives that drive effective risk management.

In financial services, assessing risk culture has been a key area of regulatory focus for some years. Outside financial services, boards should generally not need new mechanisms to oversee risk culture – it should be seen as a component of assessing and monitoring culture as required by Provision 2 of the UK Corporate Governance Code. Hence boards should leverage existing governance, risk and people information, combined with targeted qualitative insight and board judgement.

Observable drivers of behaviour

Rather than attempting to measure risk culture directly, leading practice (particularly in financial services) focuses on drivers of behaviour:

- **Purpose and strategy:** clarity on risk trade-offs
- **Leadership:** tone, challenge, openness
- **People and incentives:** what is rewarded or tolerated
- **Governance and oversight:** accountability, escalation, follow-through

This reframes risk culture as something boards can evidence and interrogate, not just describe.

Monitoring and reviewing risk culture

There is no single measure for risk culture. Boards can monitor risk culture by re-interpretating existing information flows, rather than commissioning new data. Good practice is to combine hard indicators with qualitative insight and narrative.

Board and committee papers, and meeting conduct

- Evidence of constructive challenge and how decisions balance risk and performance.
- Whether risk is embedded in strategic decision-making or treated as compliance.

Risk and audit reporting

- KRI breaches, percentage of risks and controls within appetite, repeat incidents, overdue actions and speed to remediate.
- Internal audit findings on control discipline and root causes (e.g. workarounds, overrides).
- Findings from root cause analysis and actions taken as a result.

People and conduct data

- Engagement survey themes around openness to discuss dilemmas or issues, and comfort to speak up and provide constructive challenge.
- Whistleblowing activity, themes and resolution quality.
- Non-financial misconduct trends and outcomes, such as sanctions for misconduct.
- Grievances, disciplinaries and exit data.

Direct board insight

- NED site visits and workforce engagement.
- 'Unfiltered' feedback from employees and stakeholders.

Risk culture – lessons from financial services

Financial services regulation has made risk culture more tangible by shifting the focus from stated values and policies to observable behaviours, accountability and outcomes. The core lesson for boards outside financial services is that risk culture should be assessed through evidence of how risk is understood, escalated and acted on across the organisation.

First, leadership expectations need to cascade into governance, controls and decision-making. Regulators increasingly look at the processes deployed and ask whether they are producing the right outcomes, a shift reinforced in financial services by the Consumer Duty. This means boards should focus both on whether risk procedures are followed and whether procedures are leading to better decisions, timely escalation and fair outcomes.

Second, culture becomes real when accountability is clear. Regimes such as the Senior Managers and Certification Regime (SM&CR) have required firms to allocate explicit ownership of key risks to key individuals. Ownership is then supported by risk maps, governance structures and information flows to senior management and the board. While formal enforcement of SM&CR has been limited, the perceived accountability has influenced behaviour by making responsibilities and consequences more visible.

The practical lesson is that boards need credible accountability, decision-useful management information and incentives that reinforce the desired behaviours. Without high-quality evidence and clear consequences, it is difficult to know whether the stated risk culture reflects firm practice.

Practical questions for boards

- Where are people least likely to escalate risk – and how do we know?
- What behaviours are our incentives encouraging in practice?
- What do recent incidents, audit findings or control failures tell us about underlying behaviours?
- Do we have evidence that risk information is reaching the board early enough and in a form that supports challenge?
- Where is accountability clear on paper but weak in practice?

Alex Roy
EY UK Director, Regulatory Insights Team, EY Financial Services

alex.d.roy@uk.ey.com

4.2 EY Provision 29 'how' statement reporting model

294 The board should provide a summary of how it has monitored and reviewed the effectiveness of the framework during the reporting period. This may include the type of information the board has received and reviewed; the units and individuals it has consulted with; any internal or external assurance received; and if relevant, the name of the recognised framework, standard or guideline the board has used to review the effectiveness.

Based on our analysis of ARAs, we consider that there remains room for improvement in the way the board monitoring and review process (the 'how' statement of Provision 29) is articulated.

Our reporting model should help companies create a cohesive commentary through a clearer indication of information flows from management to directors, allowing for duplication between various sections to be removed and increasing the focus on outcomes-based governance reporting. While we have attempted to make the model comprehensive, each company should take from it only what is truly material in its context.

A version of the model with reporting extracts drawn from the 2025 reporting cycle is available on request.

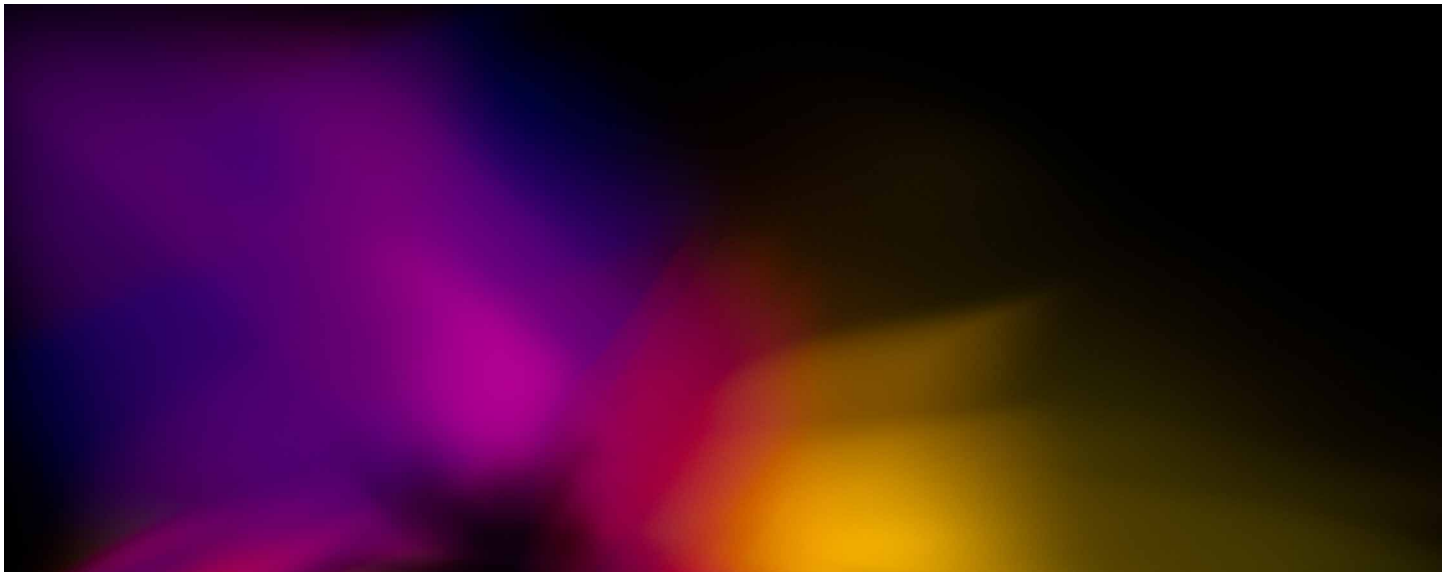
	Description of the features of the risk management and internal control framework	Company-level monitoring	Board-level monitoring	Board review
Risk governance framework				
Board	Provide clarity on the allocation of oversight responsibilities for risks and controls between board and board committee level in a summary disclosure or as part of the principal risk disclosure.	N/A	Be clear on how committees interacted on those aspects of RM&IC governance where their remits overlap.	Comment whether board and committee terms of reference were updated for changes in their remits. As part of the annual evaluation of the board (Principle L) and the formal and rigorous annual review of the performance of the board, its committees, the chair and individual directors (Provision 21) comment on: ▪ The outcome of the remit allocation being assessed. ▪ Whether directors have the necessary skills, knowledge, experience, authority and support.

<table>
<tr><th></th><th>Description of the features of the risk management and internal control framework</th><th>Company-level monitoring</th><th>Board-level monitoring</th><th>Board review</th></tr>
<tr><td>Executive</td><td>Set out any:
Core executive committees with specific risk responsibilities.
Allocated risk owners/ executive sponsors in a summary table or as part of the principal risk disclosure.</td><td colspan="2" rowspan="2">Clarify the information flows from the business to the executive and to directors, including frequency of board level reporting, to evidence how this contributes to on-going monitoring.
If including a risk management process step-by-step disclosure, disclose reporting to the board/board committees as a distinct activity, or incorporate such reporting as part of the relevant steps. Alternatively, show this at the level of each principal risk.</td><td rowspan="2">Comment on whether relevant management groups/committees, key individuals and risk owners have the necessary skills, knowledge, experience, authority and support – this can be based in in-year interactions with relevant individuals.</td></tr>
<tr><td>Business</td><td>Explain risk and control related roles by reference to the three lines model. This can be achieved through:
A graphic overview disclosure.
As part of the risk management process.
In tabular format.</td></tr>
<tr><td colspan="5">Other features of the risk management and internal control framework</td></tr>
<tr><td>Risk strategy and appetite</td><td>Explain how risk appetite is set.</td><td>Explain how management monitors whether net risks remain within risk appetite, for example by:
Disclosing the metrics that are monitored.
Setting out how tools such as risk dashboards are used.</td><td colspan="2">Confirm that directors have set and approved risk appetite.
Communicate whether the risk remained within risk appetite, and whether it was revisited towards the year-end. Where monitoring indicated that risk was outside of risk appetite, disclose how directors held management to account for addressing the situation.</td></tr>
<tr><td>Risk culture and related policies</td><td>Make clear reference to culture and conduct as part of describing the risk management and internal control framework.
When explaining the desired culture outside of the risk section, move beyond a focus on inclusion, wellbeing, etc. to address aspects relevant to risk culture.</td><td>When discussing tools such as culture dashboards, explain which data points support risk culture considerations.
Illustrate the monitoring of whistleblowing reports.</td><td colspan="2">The Provision 2 disclosure setting out how the board monitored culture and its embedding should address risk culture, including oversight of whistleblowing/speak-up arrangements and conclusions about their effectiveness, in line with Provision 6.</td></tr>
</table>

	Description of the features of the risk management and internal control framework	Company-level monitoring	Board-level monitoring	Board review
Training and communications	Reference any key policies relevant to risk management and how these are communicated to staff and what training might be required, in respect of its code of conduct.	Clarify how completion of mandatory training is monitored and enforced.		
Risk management process				
Risk identification and evaluation:	▪ To clarify definitions when using non-standard terms (e.g. key risks, material risks) include a risk taxonomy or categorisation.[2] ▪ Set out how principal risks are identified, and how emerging risks identification differs from that of principal risks. ▪ Clarify which risk attributes are reviewed when principal risks are assessed.	Set out the risks that have been identified and the outcome of their evaluation as part of the principal risk disclosure. This can include: ▪ The overall risk level, often derived from probability and impact assessment, and overall risk trend. ▪ Connectivity with emerging risks, or with other principal risks. ▪ Disclosure of velocity, or timeframe.	N/A	▪ Set out how the board monitors each specific principal risk as part of the principal risk disclosure. ▪ Set out the outcomes of directors' robust assessment of principal risks.
Risk responses:	▪ Provide an overview of the internal control framework. Set out who performs and who monitors the operation of internal controls, for example as part of the risk management process. ▪ Consider explaining how material controls are designated and how this fits into the broader response framework. ▪ Address the requirements of DTR 7.2.5 to include a description of the main features of the internal control and risk management systems in relation to the financial reporting process.	▪ Set out the risk-specific responses as part of the principal risk disclosure. In doing so avoid implying that all mitigations are controls, for example by categorising the responses. ▪ Be clear where responses were specific to the year, and set out where additional measures will be implemented going forward.	Set out the additional sources of insight available to directors, such as: ▪ Overview of activities undertaken by internal audit by reference to individual principal risks. ▪ External certifications. ▪ Other sources of external confidence. ▪ Provide examples of how the board obtained assurance across a variety of sources.	

2. In our sample, 28% of companies used terms such as 'key risks' or 'material risks' in the context of material control identification without providing a risk taxonomy to explain how these terms align with principal risks.

	Description of the features of the risk management and internal control framework	Company-level monitoring	Board-level monitoring	Board review
Monitoring effecti-veness:	Set out what is monitored in respect of specific risks as part of the principal risk disclosure.		Comment on any actions requested to improve the effectiveness of the company-level monitoring activities.	▪ Where relevant, comment on how actions arising from prior period and in-year findings were progressed or closed out. ▪ Comment clearly on whether any final updates or representations were obtained to move from monitoring to year-end review. ▪ Specifically, comment on how the audit committee reviewed the company's controls over financial reporting, distinguishing monitoring and review activities.
			If other areas of the annual report clearly set out what management does and what sources of insights are reported to the board and its committees, the board and committee reports can focus on outcomes organised by the most material themes, demonstrating how various sources of insights are used in combination to challenge management's conclusions.	



5. Illustrative 'how' statement and declaration

In its January 2026 Provision 29 Mythbuster, the FRC emphasised the following:

How should the declaration be worded?

The FRC will not be providing any wording for declarations, as companies will choose to approach this in different ways. As long as **the declaration** is clearly signposted in your annual report and the board demonstrates oversight and confidence in the material controls, this would constitute compliance with the second bullet of the Provision.

How long should reporting under Provision 29 be?

The declaration is only one element of the reporting, and so the report should also include **commentary on the monitoring and review process**, as well as an explanation of how the board reached its decision. In most cases, we expect the report to be no longer than two pages. It is essential that the reporting remains proportionate and concise.

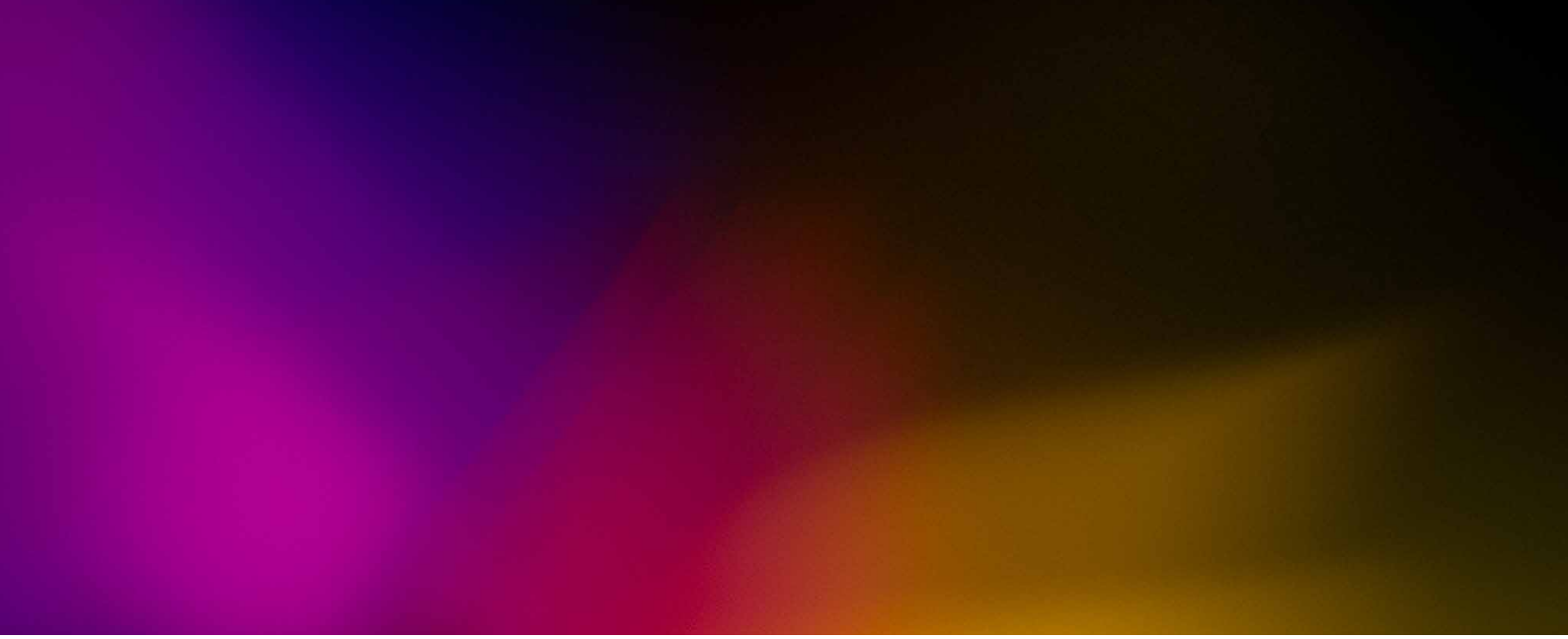
Below is an illustrative draft of the commentary on the monitoring and review process, aligned with our reporting model, and a 'clean' declaration that can serve as an inspiration. It sets out the information flows from management to directors and between board committees all the way to the board, in a manner like the approach demonstrated by Next (Example 22). The example below is intentionally comprehensive; companies should tailor it to reflect what is material in their circumstances.

5.1 The Board statement and declaration

The risk management and internal control framework established by the Board is described in the risk management section. The framework includes, among other elements, procedures to identify principal risks, material controls over those risks as well as procedures to identify and manage emerging risks.

Having delegated some aspects of the role to its committees, as described in the overview of the governance framework, the Board retains ultimate responsibility for the risk management and internal control framework. The Board has maintained this framework throughout the year and monitored its effectiveness through:

- The risk monitoring activities conducted by the Board's committees, most notably the **Audit Committee**, as set out in the committees' reports.
- Its direct engagement with **risk owners** regarding those principal risks overseen directly by the board, namely [XXX].
- Its culture monitoring activities, described on page [X], which included monitoring of the **risk culture** and routine assessments of **speak-up** arrangements and reports arising from their operation.



The Board confirms that it carried out a **robust assessment of the company's emerging and principal risks** and evaluated the quality and frequency of risk management reporting. It remains satisfied that the design of the risk management and internal control framework remains appropriate considering the changes to the risk profile described in [xxx].

Furthermore, the Board carried out a **review of the operating effectiveness of the framework**, including its material controls, which involved receiving and interrogating:

- Recommendations on the material control effectiveness declaration from the Audit Committee.
- Self-attestations from all the principal risk owners.
- Outcomes of the viability assessment.
- [Other as relevant, for example, insurance arrangements].

The Board also reviewed the adequacy of **policies** [X, Y, Z] and ensured that they were appropriately updated to address regulatory and other changes. Furthermore, the Board also ensured that the **terms of reference of its committees** adequately reflect their responsibilities in respect of the risk management and internal control framework and that the committees have the necessary resource and expertise to deal with those responsibilities.

The monitoring activities combined with the year-end review provided the Board with sufficient appropriate evidence and reasonable confidence to determine and declare that all material controls were effective as at the balance sheet date. The Board's declaration is subject to the inherent limitations of any system of internal control and assurance, which is designed to provide reasonable, rather than absolute, assurance.

5.2 The Audit Committee statement

Throughout the year, the Audit Committee monitored the risk management and internal control framework through insights obtained from its oversight of **company-level monitoring**, described in the risk management section, supplemented with **additional sources of insights**, of which the following were most significant:

- Key risk indicator reporting.
- Ad hoc escalations of near misses, incidents and other risks, together with associated pathways to remediation.
- Risk dashboards, which included updates on principal risks and responses, and regular reporting on principal risks from designated risk owners or the Chief Risk Officer.
- Progress reports against previous internal audit findings.
- Outcomes of investigations into whistleblowing reports related to incidents of suspected fraud.

As a result of its monitoring, the Audit Committee was satisfied that management had put in place robust action plans with appropriate target dates to address any areas for enhancement and that sufficient resources were in place to deliver on these. For example, [provide some areas of enhancement if relevant].

The Audit Committee also undertook **a formal review** of the risk management and internal control framework. This review drew on multiple sources across the three lines, including:

- Self-assessments and validation exercises undertaken by the first and second-lines.
- Risk deep-dives indicated as part of principal risk reporting.
- Self-attestations from risk owners and material control owners, as well as entity/business unit attestations on adherence to the group framework.
- Delivery of the approved internal audit plan, which is set out in [the risk management section].
- Outcomes of the execution of other elements of the assurance plan, [e.g. input from third parties, testing results undertaken on attestations].

In addition, the Audit Committee sought input from the Technology Committee.

The Audit Committee also obtained an understanding of remediation progress in areas identified through monitoring and tracked management action plans and overdue items. It is satisfied that, at the year-end, any significant failings or weaknesses related to material controls identified as part of monitoring activities had been or were being adequately remediated.

Separately from activities related to principal risks, the Audit Committee also monitored and reviewed the company's internal controls over financial reporting. This included:

- Reporting on the design and operational effectiveness of IT controls supporting financial systems and processes from the second-line and Internal Audit.
- Assessing and monitoring management responses to key external audit findings.
- Overseeing financial results compared with the plan.
- Regular reporting from the CFO on enhancements to the financial reporting processes, including improvements to documentation, testing and monitoring of key controls.

The work undertaken provided the Committee with reasonable confidence that key financial reporting and control processes were consistently applied across the group. A description of the main features of the internal control and risk management systems in relation to the financial reporting process as required by Disclosure Guidance and Transparency Rule 7.2.5 is set out in [xxx].

Based on the review, the Audit Committee made recommendations to the Board on the material control effectiveness declaration.

5.3 The 'other committee' statement

The Technology Committee contributes to the oversight of the cybersecurity principal risk. During the year, the committee:

- Oversaw the results of the annual penetration testing and the cyber simulation exercise and the testing of the Cyber Incident Response Plan.
- Was appraised on a regular basis about the outcomes of the continuous IT system vulnerability scanning and regular phishing simulations aimed at proactively identifying and addressing weaknesses.
- Monitored completion rates of the cyber-awareness training designed to support colleagues in recognising and responding to threats.
- Considered the output of an external assessment of the group's cybersecurity control environment.

The Committee also reviewed management's work to identify critical business services and strengthen recovery planning, as part of improving the group's operational resilience. The Committee recommended, and management agreed, to update the membership of the Group Business Continuity team to reflect outcomes of this work.

The Committee held a joint session with the Audit Committee to support the latter's year-end effectiveness review of the risk management and internal control framework, providing its views on cyber risk and the effectiveness of related responses.

5.4 When a material control did not operate effectively as at the year-end

As the deadline for the first declarations approaches, conversations about the consequences of disclosing that a material control did not operate effectively as at the year-end are intensifying.

Many companies, such as ITV, Aberdeen, Playtech and Rolls-Royce, already disclose where the need for enhancements to the risk management and internal control framework was identified and what steps were undertaken to implement them. These disclosures can be seen to demonstrate the effectiveness of management and board-level monitoring of the framework and a continuous-improvement mindset.

However, given what material controls are intended to achieve, having to declare that one did not operate effectively as at the year-end is more problematic. It could raise questions on whether:

- Monitoring activities did not achieve their objectives because they did not operate as intended.
- Risks with the potential to threaten the viability of the company or its access to capital were not appropriately managed.

And, ultimately, whether those charged with governance failed to adequately discharge their duties.

For these reasons, if the declaration is not 'clean', directors should consider providing disclosures beyond those explicitly stipulated in the third bullet of Provision 29. It is not possible to foresee every possible scenario that could lead to this situation; however, some examples for consideration could include:

- If issues with a material control were identified during the year but had not been sufficiently remediated by the year-end, directors may wish to make this point clear when discussing the outcomes of the framework monitoring. They may also want to discuss what compensating measures were put in place during the remediation period to address the resulting risk exposure.
- If monitoring had not picked up the issues, then in addition to setting out the actions taken or planned to remediate the material control, directors may want to specify how monitoring activities will be enhanced going forward and whether any compensating measures have been effected in the meantime.

5.5 Questions the board should be asking

Once drafted, the risk management section and 'how' statement should be scrutinised by directors to ensure they fairly and accurately reflect the activities undertaken during the year and the position at year-end, without overstating strengths or omitting material elements.

As part of their fair, balanced and understandable assessment, directors may wish to consider the following questions:

- Do the principal risk disclosures align with information provided to support their robust assessment under Provision 28?
- Are statements made in relation to risk appetite (and operating within it, where relevant) supportable?
- Are management's monitoring and review activities clearly distinguishable from those of the directors?
- Is it clear whether the governance activities described were undertaken during the year, rather than reading like boilerplate or process narrative?
- Is the governance reporting sufficiently outcomes-focused?

6. Extended case study: Material controls over geopolitical risk

Already in the 2025 reporting cycle, 61% of the FTSE 350 identified geopolitical risk (or an equivalent) as a principal risk, with many others describing it as an emerging risk. However, given the velocity and inherent unpredictability of geopolitical developments, disclosures often suggest that – even where geopolitics is classified as a principal risk – an organisation's responses are similar to those applied to emerging risks.

Mitigations disclosed in ARAs are a mix of adaptive and reactive measures, commonly including:

- Horizon scanning and exposure mapping
- Event monitoring, intelligence and early warning
- Government and stakeholder engagement, including advocacy
- Scenario analysis and stress testing
- Crisis and incident management
- Supply chain and operational dependency management
- Funding flexibility, liquidity and treasury management
- Cost, pricing and margin management
- Business continuity, contingency planning and operational resilience
- Regulatory and compliance management
- Security, safety and asset protection

Since year-end, geopolitical risk has escalated sharply. In the EY-Parthenon May 2026 CEO Outlook, 56% of global CEOs identified geopolitical tensions, instability and conflict as the key near-term risk, up markedly from 28% in September 2025, when technology disruption and AI, combined with access to talent, were top of mind for the C-suite.

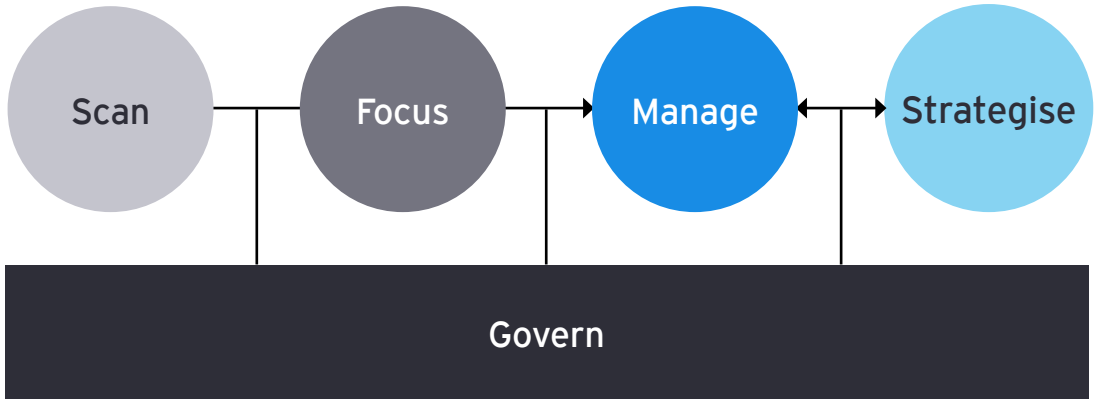
As boards reassess principal risks during 2026, it would not be surprising if geopolitical risk is either elevated to principal risk status or, where already classified as such, increased in severity. In either case, a recalibration of the organisation's response will be required to reconsider how resilience is defined in the context of severe, sustained geopolitical disruption.

In our view considering such re-calibration effort against the key elements of the EY geostrategy framework for strategic political risk management would help ensure effective structuring:

Scan
Identify and monitor political risks for opportunities and challenges, with an assessment of likelihood.

Focus
Focus on how the risks identified in the scan will affect the company in specific and measurable ways across its functions, business units and geographic footprint, with clarity on the impact on performance metrics.

Manage
Evaluate the relationship between the likelihood of risks occurring and their impact to determine how to actively manage them.



Govern
Establish appropriate structures based on the fundamentals of ownership, communication and trust.

This means assessing how roles and responsibility for geostrategic risk management are assigned, and considering what information enables board-level monitoring of geopolitical exposure and how information flows through the organisation to help decision-makers frame their decision points. Doing this well will ultimately enhance trust across the organisation.

Strategise
Incorporate political risk analysis into operations and strategy.

This primarily relates to the strategic levers available to companies in responding to a changing geopolitical environment. In practice, this increasingly centres on diversification and dependency management across markets, supply chains, assets and revenue streams.

While there are many overlapping elements between Manage and Strategise activities, the latter's focus should also extend beyond the current business landscape to seize opportunities rather than simply protect against unforeseen changes.

6.1 Material controls linked to geopolitical risk and their effectiveness

When companies were first determining their material control populations around 12 to 18 months ago, a common conclusion was that there were few, if any, material controls addressing geopolitical risk. This reflected the view that, while such risks may be unavoidable and highly impactful, they are largely outside the organisation's direct control. However, as organisations have continued to refine their overall approach to Provision 29, activities that might previously have been characterised solely as 'responses' are increasingly being elevated to material control status, including in respect of geopolitics. Based on our engagement, these most commonly include horizon scanning, scenario modelling and stress testing, and business continuity planning.

Material controls that, in practice, operate primarily as mechanisms for identifying risks or shaping responses, rather than preventing or detecting risk events themselves, create a particular challenge in the context of the declaration. Unlike more traditional controls, those relating to geopolitical risk cannot be evaluated solely through periodic testing or assurance activities. Their effectiveness is inherently dependent on factors such as the timeliness of response, the quality of decision-making and the degree of coordination across the organisation. This raises a fundamental question as to how conclusions can be drawn on the effectiveness of such material controls where the ultimate efficacy of the response may only be evidenced when a geopolitical event occurs and the response executed in practice.

One of the ways this challenge can be addressed is through a greater focus on the controls over the design, maintenance and awareness of those responses, and over the organisation's readiness to deploy them, rather than on the responses themselves. This is similar to the approach we proposed in The Goldilocks phase and beyond for addressing the effectiveness of entity-level material controls.

Element of the entity-level control	Equivalent element of the geopolitical material control
Documented policy or standard	Design and maintenance
Communication and training	Awareness
Monitoring of adherence	Organisational readiness

We apply this framing to illustrate how the most common material controls in respect of geopolitical risk – horizon scanning, scenario modelling and stress testing, and business continuity planning – can be assessed for effectiveness.

6.2 Horizon scanning

Many companies already deploy horizon scanning as part of their emerging risk identification processes. In the context of geopolitical risk, this is typically supported by ongoing government and broader stakeholder engagement, providing insight into policy direction and regulatory intent, alongside event monitoring and intelligence capabilities that enable real-time situational awareness and timely responsiveness.

Element	Example effectiveness consideration

Design and maintenance	▪ The approach to horizon scanning has been approved by those with an appropriate level of seniority and there is a clear linkage to the business strategy.
	▪ The approach to horizon scanning is up to date, for example:
	  ▪ Boundaries for the scan have been updated for any recent changes to the business.
	  ▪ Sources of geopolitical information used in the scan are reviewed on a regular basis for adequacy. Arrangements to access external specialist expertise for intelligence on fast-moving developments to supplement and stress test internal work have been considered or are in place.
	  ▪ Frequency of horizon scanning is responsive to the levels and volatility of the geopolitical risk.
	▪ There is a documented output of the horizon scan that includes a clear assessment of risks using both qualitative and quantitative analysis (e.g. metrics to track risk trends over time and enable scenario modelling).

Awareness	▪ Outputs from scanning are communicated to the business, with clarity on actions needed, for example, in refining or adapting mitigation strategies. ▪ Outputs are reflected in key risk indicator dashboards. ▪ There are clearly defined triggers for when rapid escalation is required.
Organisational readiness	▪ There is clear ownership of actions and follow-up on completion.

“

Local-level intelligence, from business units, functions and geographies, should be brought together at the group level and aligned with enterprise-wide priorities. Horizon scanning should match how decisions are made: frequent, practical updates for operational teams, and clear input into board-level risk analysis to guide major strategic decisions. This process and the communications around it must also be two-way, with direct access between the central analytical team and both the C-suite and the board, to support both ongoing insight sharing and targeted strategic questions.

Courtney Rickert McCaffrey
EY Global Geostrategy Insights Leader
courtney.r.mccaffrey@ey.com

6.3 Scenario modelling and stress testing

In assessing the effectiveness of scenario modelling, it is not sufficient to ascertain whether a scenario has been considered; what matters is whether the organisation has demonstrated that it could respond effectively if the scenario crystallised.

This challenge is well illustrated by the long-discussed risk of disruption in the Strait of Hormuz. While the potential closure of the Strait has featured in industry risk assessments for many years, organisations have generally not translated this into meaningful response plans, particularly with regard to the indirect, knock-on impacts on downstream industries, largely because the scenario was viewed as low probability. As one CEO in the oil and gas industry candidly acknowledged, "we are stupid in our industry" companies have recognised the risk but have not consistently converted that awareness into operational preparedness.

As a result, scenario modelling needs to be complemented by the development and refinement of response playbooks, helping to translate insight into actionable and coordinated management responses.

In practice, many companies are moving beyond traditional 'desktop' scenario analysis towards more dynamic 'mobilised' scenarios that actively involve relevant functions and decision makers. These exercises test whether geopolitical risks are well understood in practice, whether controls are appropriately designed, and whether governance arrangements, resources and response plans are capable of being executed under real-world conditions.

Element	Example effectiveness consideration

Design and maintenance	▪ The scenarios have been approved by those with an appropriate level of seniority.
	▪ Time horizons have been clearly articulated.
	▪ The scenarios are up to date, for example:
	  ▪ They reflect any recent changes to the business.
	  ▪ They reflect the geopolitics-related outputs from the horizon scan.
	  ▪ They include consideration of 'grey rhinos'.[3]
	▪ Modelling of the scenarios is updated on a regular basis and aligned with planning cycles.

Awareness	▪ Consequences and outcomes of scenarios are communicated to relevant business units and functions and incorporated into risk modelling.
Organisational readiness	▪ Risk response playbooks are created and meaningfully stress tested under realistic time pressure with C-suite participation. ▪ No-regret moves to boost resilience are implemented.

"

Integrating geopolitical risk into strategy requires a structured approach. It begins with stress-testing the macro assumptions underpinning the business model and modelling how performance degrades under alternative conditions. Organisations should then identify and prioritise their most critical vulnerabilities across operations, supply chains and market access, focusing on those most likely to shift over a defined time horizon. Strategic planning should be anchored in a set of differentiated scenarios that reflect fundamentally distinct geopolitical trajectories, rather than incremental variations on a baseline. The EY Geostrategic Business Group supports this end-to-end process, combining its Geostrategic Outlook, sector expertise and proprietary globalisation scenarios to translate geopolitical uncertainty into actionable strategic, operational and crisis-readiness decisions.

Oliver Jones
EY-Parthenon Geostrategy Leader & Global Leader in Client Insights and Research
oliver.jones@uk.ey.com

3. Grey rhinos are 'known unknowns'. They are more plentiful and expected, charging in plain sight, and with a significantly wider impact yet often ignored. These charging grey rhinos represent the risks that boards should proactively prioritise within their enterprise risk management, i.e. anticipate and adapt rather than react. By contrast black swans are 'unknown unknowns'. They can be catastrophic, but they are unique, rare, impossible to predict, and outside an organisation's control.

6.4 Business continuity planning (BCP)

While some companies treat their strategic planning process or business plan as a material control for geopolitical risk, this remains less common at present. What is becoming more prevalent is a shift towards greater emphasis on resilience. As a result, business continuity and operational resilience planning is increasingly being elevated and treated as a material control.

This typically involves assessing geopolitical risk exposure and response maturity relative to peers — by sector, geography and scale — and using this insight to define a target level of resilience aligned with the organisation's risk appetite. This in turn can iteratively inform scenario analysis, for example by ensuring that modelling factors in critical business services by geography.

Element	Example effectiveness consideration
Design and maintenance	▪ The BCP is prepared with input from representatives of critical functions. ▪ The BCP has been approved by those with an appropriate level of seniority. ▪ The BCP is regularly updated, including for outcomes of scenario modelling.
Awareness	▪ Clear communication, decision and escalation protocols have been established, including with relevant third parties. ▪ Training for general staff on emergency protocols is in place.
Organisational readiness	▪ BCP is regularly tested through simulations or tabletop exercises. ▪ Testing involves senior management to rehearse incidents, test decision-making roles and escalation paths. Employee and external communication channels have been tested.

Severn Trent (**Example 23**) includes detailed disclosures about its business continuity activities. In addition, it separately notes that as part of its continued focus on operational resilience, its Board participated in a live cyber incident simulation. This replicated the pressure, pace and uncertainty of a real cyber attack, enabling Board members to test decision making, escalation routes, crisis communication and regulatory reporting in a realistic environment.

6.5 Considerations for the final stretch

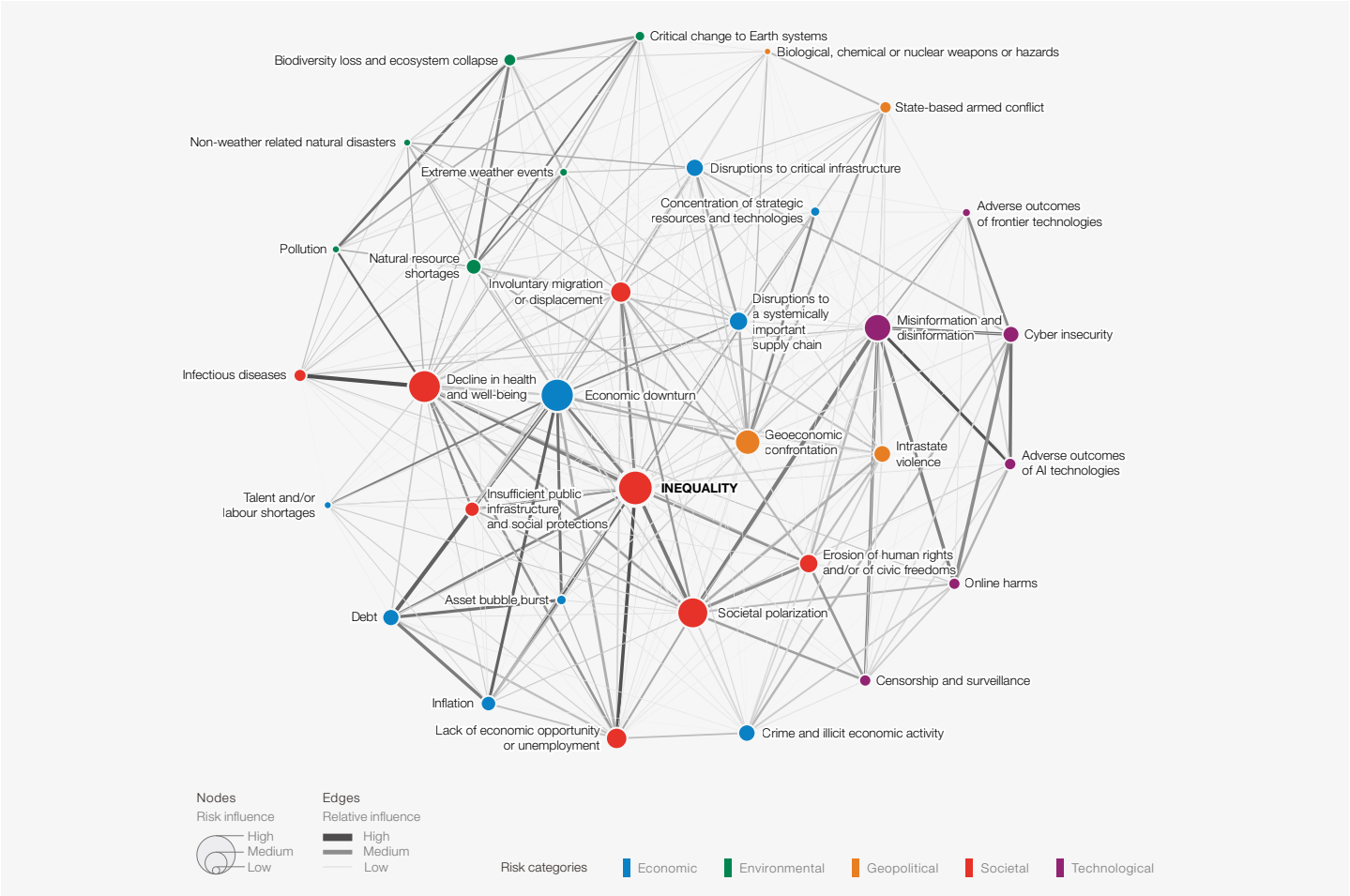
Many companies regard geopolitics as a cross-cutting risk driver. Geopolitics creates, amplifies or accelerates other operational, economic and security risks. Most notably, the World Economic Forum (WEF) **Global Cybersecurity Outlook 2026** identifies geopolitical fragmentation, alongside artificial intelligence and supply-chain complexity, as one of the principal forces reshaping the cyber risk landscape.

> “
>
> Geopolitical instability and armed conflicts are reshaping the cyberthreat landscape, creating complex and unpredictable conditions for organizations. As global fragmentation deepens — driven by conflicts, sanctions and technological rivalry — cybersecurity is emerging as a critical extension of geopolitical competition.
>
> Global Cybersecurity Outlook 2026

Geoeconomic confrontation refers to a form of geopolitical risk in which states use economic tools – such as trade policy, sanctions, investment restrictions and control of supply chains – as instruments of strategic competition to advance political or security objectives. Rather than manifesting through direct military conflict, it arises from the deliberate ‘weaponisation’ of economic interdependence, as countries seek to constrain rivals.

According to the **WEF Global Risks Report 2026**, geoeconomic confrontation has emerged as the most severe risk over the next two years. The report highlights that the centrality of geoeconomic confrontation in the global risk landscape threatens the foundations of an increasingly interconnected global economy.

This heightens the need for companies to consider whether their evaluation of geopolitical risk should trigger a reassessment of the adequacy of material controls over interconnected risks, and whether existing responses are sufficiently dynamic to remain effective as conditions evolve.



WEF Global Risks Report 2026, Figure 6

6.6 What comes next

To date, we have not observed companies treating the following as material controls. However, as geopolitical volatility appears set to become the new normal, it would not be surprising if they begin to be considered as such.

6.6.1 Executive-level geostrategic risk committee

While many annual reports reference oversight by the board or its risk committee and involvement of corporate affairs, legal, compliance and regulatory teams, we have not come across references to standing geostrategic risk committees, although our engagement indicates that they do exist. In the 2025 Geostrategy in Practice survey, all of the companies interviewed indicated that they had altered their strategic investment plans as a result of political risks over the past 24 months. In the same survey, however, fewer than one-third of executives reported that their company does this on a proactive basis – meaning that, in most cases, companies respond to political risk only as events arise.

Where geopolitics is a principal risk and no such committee exists already, companies should consider the merits of establishing one with a remit to address the risk proactively. While not itself a material control at present, establishing one could provide a valuable opportunity to reassess whether the information provided to directors to support ongoing monitoring of the risk management and internal control framework is sufficiently robust. In particular, this may include considering whether relevant metrics on geopolitical exposure – such as supply-chain concentration by geography or dependency on higher risk jurisdictions – are routinely reported to enable informed oversight and challenge.

As organisations start to transition into business as usual after the first declaration, such a committee could evolve into an oversight cluster control that, amongst other things, oversees the controls described above – horizon scanning, scenario modelling and stress testing, and business continuity planning.

> “
>
> The Committee believes boards should take a more structured approach by assigning responsibility for geopolitical oversight, undertaking regular scenario planning, and ensuring they understand both the risks and the opportunities created by a changing global landscape. In an increasingly fragmented world, geopolitical awareness is becoming a source of competitive advantage.
>
> Three Priorities for the Board of the Future,
> The ICGN Future Leaders Committee

6.6.2 Minimum viable company

The resilience of organisations is becoming increasingly important, with major business disruptions and outages being ever more common. During times of severe, mass disruption, when in emergency mode, businesses need to be able to continue to operate to survive. This has driven a shift in thinking and approach when responding to major outages, away from solely recovering to normal operations as quickly as possible, towards the explicit prioritisation of what must be preserved or recovered first to stop the company grinding to a prolonged halt – the so-called **minimum viable company (MVC).**

From our review of disclosures, there are a handful of references to the MVC concept. The audit committee of Domino's Pizza discussed and challenged the identification of business-critical systems and which of these comprise a minimum viable trading platform, with a specific focus on ensuring recovery processes are well-established and failover testing. As part of improving the group's operational resilience, the audit committee of ITV reviewed management's work to identify critical business services – MVC – and strengthen recovery planning, including the ability to respond to scenarios where key systems or third-party services are unavailable.

MVC is not a documented plan, but a defined target operating state. While related to business continuity and disaster response plans, it is distinctly different. At a high level, these plans seek to answer the question of how to restore normal operations; they are a plan to execute, to direct the journey, to recover. The MVC, on the other hand, is a critical stop on that journey that underpins the future recovery activities. Once MVC is established, organisations can focus on rebuilding in a controlled way, limiting the overall impact of the crisis. MVC sets out the minimum set of services, capabilities, dependencies and resources that must remain operational for an organisation to continue functioning, meet its obligations, and support a controlled recovery under severe disruption. Put simply, it asks: *what is the minimum version of this organisation that must continue to operate under sustained disruption?*

> “
>
> On a practical level, to deliver a successful MVC, organisations need to focus on getting the following two key aspects right:
>
> 1. Ensuring strong inter-departmental collaboration to ensure that the business's MVC is truly understood and accurately reflects the needs of the business. This is paramount to enable the effective recovery and preservation of the MVC.
> 2. Extending the analysis of what the MVC is to the supply chain to identify and account for dependencies on other organisations that impact effective recovery.

Andrew Napier
EY UK Director
Technology Risk
anapier@uk.ey.com

Resilience, in this context, is no longer defined by the ability to prevent failure, but by the ability to withstand it – to prioritise crisis response in a controlled way, maintain critical operations, and recover predictably under pressure. It requires organisations to anticipate, absorb and adapt to complex, interconnected risks, not only those arising from cyber threats. Over time, having a defined MVC has the potential to become a material control in managing high impact risks that sit, at least in part, outside an organisation's direct control.

Appendix:

Annual report extracts

Example 1

Energean 2025 ARA, p. 107, 109

Preparation for the revised Provision 29 of the 2024 UK Corporate Governance Code

A major area of focus in 2025 was the Committee's preparation for the enhanced requirements of the New Provision 29, which takes effect for financial years beginning on or after 1 January 2026. Under the New Provision 29, the Board will be required to provide a formal declaration on the effectiveness of the Company's material controls, covering financial, operational, reporting and compliance controls.

Building on the preparatory work commenced in 2024, the Committee oversaw the following activities during 2025:

- The focus group led by the Head of Compliance and the Head of Internal Audit continued and expanded its work, conducting walkthroughs of core business processes across selected areas of the business, as well as ensuring that appropriate training and awareness is provided at the Board and senior management level.
- The Committee endorsed management's framework for identifying and defining "material controls" in alignment with the Group's principal risks, considering guidance from the FRC and best practices.
- Risk Pilot sessions were conducted with the objectives of: breaking down the Organisation's key risks into their underlying causes/sub-risks, identifying relevant Key Risk Indicators ("**KRIs**"), defining the controls in place, determining the periodic testing and assurance activities employed to monitor and validate control effectiveness, obtaining feedback regarding third party assurance and reviewing activities that enhance risk coverage.

The Committee oversaw the conduct of two Risk Pilots covering project delay risk and cyber risk, and agreed that further pilots would be progressed during 2026 in areas including liquidity risk, and legal and regulatory risk.

The Committee also supported continued use of a structured verification process for controls-related statements in the Annual Report to ensure that key claims are supported by evidence and a clear audit trail exists for external scrutiny.

The Committee is satisfied that the Group is well advanced in its preparations and is on track to comply with the enhanced New Provision 29 requirements for the financial year beginning 1 January 2026.

The deep dive and Risk Pilot sessions conducted throughout the year on the following topics proved to be an effective means of making progress and resolving matters efficiently:

- JV and non-operated asset management practices for our Italian Operations
- IT & Cyber security
- Katlan development project
- Egypt concession merger and receivables management.

The Committee also held several discussions regarding readiness for the New Provision 29. During 2025, the following actions were undertaken:

- Preparation of the relevant framework, including the overall approach, assignment of responsibilities and development of timelines.
- Development of the Key Controls Repository, which was validated through a dedicated Board survey.
- Coordination of two Risk-Pilot sessions to strengthen the evidence base and enhance control-testing discipline in line with the requirements of the New Provision 29.

Source: 2025 Energean ARA

Example 2

Ocado 2025 ARA (November), p. 85, 127-129

Our approach
During FY25, significant progress has been made in preparing for compliance with Provision 29. The Committee and the Risk Committee have received regular updates on the timeline to compliance, reviewed an initial assessment of material controls and assurance map (an overview of where material control assurance will be sourced from) and discussed how to strengthen the current control environment and the associated resource requirements. In FY26, the Committees will continue to review the assurance activities ahead of a "dry run" later in the year.

Governance frameworks continue to be refined, and existing governance and committees will be refreshed to ensure they are reviewing material controls and strengthening any gaps, to make sure that the Board has the requisite level of confidence in time to make its annual declaration on the effectiveness of the material controls.

Assurance
Current assurance activities across first, second, third and fourth lines (see page 84) have been mapped against the material controls. An assessment of the strength of current assurance activities and any potential gaps is ongoing and will continue into FY26.

Received regular updates on the timeline to compliance with Provision 29 of the Code, including control assurance and effectiveness summaries, and oversaw the programme to strengthen documentation, testing and reporting to support the Board's future declaration.

We reported in 2024 that a cross-functional team had been established to prepare for the upcoming changes to the UK Corporate Governance Code. Since then, the team has made strong progress in developing the structures and visibility needed to meet the new expectations under Provision 29. Regular updates have been provided to the Risk and Audit Committees, which have overseen the continued strengthening of governance frameworks and alignment of committee responsibilities to ensure material controls are appropriately reviewed.

Identifying our material controls
Materiality has been informed by FRC guidance and the Company's principal risks and risk appetite (see pages 84-94 for further information on our risk appetite framework and governance process). The defined material controls are linked to the principal risks and additionally cover financial, IT general controls and non-financial reporting.

A number of controls were already monitored by the Audit Committee (financial and IT general controls) and, during the year, the Committee received updates on the progress made by management to remediate and improve the controls.

Key milestones to compliance

Date	Milestone	Progress
Jan 2024	FRC published the Code and supporting guidance.	Completed
FY25	Materials Controls Working Group created, principal risks reviewed and confirmed they remain appropriate, materiality definition agreed, material controls defined and initial assurance proposal reviewed by Risk Committee and Audit Committee.	Completed
Jan and Feb 2026	Effectiveness assessment of material controls undertaken as part of the year-end principal risk review and reported to the Risk and Audit Committees.	Completed
H1 2026	Governance Committees Terms of Reference and governance to be refreshed to ensure governance of principal risks and material controls is appropriate.	In progress
FY26	Control owners continue to monitor controls and control evidence. Risk and Audit Committees review the outcome of the 'dry run' and draft Board declaration.	Not started
FY27	Perform and monitor Code assurance activities, and work to close any control gaps. Embed controls reviews into business as usual.	Not started
Feb 2028	Annual Report & Accounts for FY27 to include the Board's declaration on the effectiveness of the Company's material controls.	Not started

Key activities of the Committee during FY25:

- Received updates on core emerging regulations and the evolving risk landscape, including tariffs, non-financial reporting and sector-specific digital and data requirements, and ensured that priorities, ownership and delivery plans were clearly defined and agreed.
- Received regular updates on the timeline to compliance with Provision 29 of the Code, including control assurance and effectiveness summaries, and oversaw the programme to strengthen documentation, testing and reporting to support the Board's future declaration.
- Reviewed and approved the updated Fraud Control Plan and wider fraud prevention compliance framework updates, developed in light of the new "failure to prevent fraud" offence introduced under the ECCTA. It received assurance mapping against ECCTA guidance and monitored progress on completed and outstanding actions.
- Carried out a robust assessment of the Group's principal and emerging risks, including those that could threaten its future performance, business model, solvency or liquidity, and reviewed the Group's approach to risk monitoring.
- Discussed the Cybersecurity & data risk appetite, exploring risk appetite levels across multiple cyber domains. This remains an area of continued discussion.
- In relation to financial risks, reviewed reports from management on the financial control environment, specifically noting progress on remediating deficiencies raised in the FY24 external audit management letter. The Committee discussed the results of the FY25 testing programme and the implementation of new processes to strengthen the control environment, such as standardised action planning. The approach was enhanced to support a controls-based audit, with a risk-based plan defined for the year ahead to include material controls testing in preparation for the Code.
- Reviewed management's approach to identifying and managing risks, discussed with management its programme of work to strengthen the maturity of the Group's risk management and internal control framework, and recommended enhancements.

Source: 2025 Ocado ARA

Example 3

Bunzl 2025 ARA, p. 103

Preparation for compliance with Provision 29 of the 2024 Code

The updated Provision 29, which applies to financial years beginning on or after 1 January 2026, requires boards to make an annual declaration in the Annual Report as to the effectiveness of all material controls as at the balance sheet date. This covers controls relating to financial and non-financial reporting, operational activities, and compliance. The declaration must also include 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.

Throughout the year, the Committee continued to oversee management's preparations to ensure readiness for compliance with Provision 29. This work, examples of which are set out below, has focused on clearly defining and identifying material controls, enhancing their design and operation, and embedding year-round monitoring to support robust, meaningful reporting.

Review of the Material Controls Risk and Control Matrix ('RACM')
The Committee oversaw a comprehensive review of the RACM to assess its alignment with the Group's principal risks and associated reporting processes, drawing on internal audit testing and management attestations. The findings were presented to the Committee and resulted in amendments to two controls and the addition of one new control. The review also identified a small number of opportunities to further strengthen certain processes. Work with control owners commenced in 2025 to address these enhancements and perform dry-run testing of control effectiveness, supported by a focused review conducted by the internal audit team.

Adoption of a Material Controls Policy
The Committee considered and recommended to the Board for approval a new Material Controls Policy that: (i) sets out the methodology for identifying and managing material controls (criteria, linkage to principal risks and disclosures); (ii) aligns the Material Controls Policy with the existing Risk Management Policy; and (iii) integrates the Internal Controls Essentials programme and similar functional frameworks to avoid duplication and to standardise evidence expectations.

Covering financial, operational, reporting and compliance domains, the Material Controls Policy also clarifies accountability among management, risk owners and the Committee for ongoing monitoring and the annual review of material controls.

Governance updates
To reflect the enhanced responsibilities introduced by Provision 29, the Committee's terms of reference were updated in 2025 to explicitly reference material controls and the associated Board declaration. This update has strengthened the governance structure by clearly delegating authority to the Committee and expanding its remit in relation to risk management and internal controls.

The Committee is satisfied that the prepatory work undertaken during the year has further strengthened the Group's control environment and enhanced the visibility and oversight of material controls. Based on the progress achieved to date, and the continued work planned for 2026, the Committee is confident that the Board will be well positioned to make the required declaration under Provision 29 when it becomes applicable.

CYBER: AI GOVERNANCE

As part of the Committee's ongoing prioritisation of cyber and information security, it also oversaw Bunzl's approach to AI during 2025. With the Committee's support, the Group strengthened its AI governance through the adoption of updated policies, enhanced risk management measures, and reinforced oversight. The Company's AI policy defines acceptable use and governs the use of company, supplier, and customer data within external Generative AI tools. In addition, a Data Security & AI Risk Approach was implemented across the Group to address key risks, including privacy, cyber security, regulatory compliance, and third party AI usage.

BUNZL'S CYBER SECURITY RISK MITIGATION FRAMEWORK

Identify Know what we have, what we do, and what's important	• Asset Management • Business Environment • Governance	• Risk Assessment • Risk Management
Protect Stop the things we should and do the basics well	• Identity Management • Awareness and Training	• Data Security • Information Protection
Detect Quickly, simply, and efficiently find what needs to be stopped	• Anomalies and Events • Detection Processes	• Security • Continuous Monitoring
Respond Implement processes to deal with events in real time	• Analysis • Mitigation • Improvements	• Communications • Response Planning
Recover Return to known good state and focus on continuous improvement	• Disaster Recovery • Continuous Improvement	• Communications

Source: 2025 Bunzl ARA

Example 4

Tesco 2026 ARA, p. 61, 83

Spotlight on:

Code readiness

Provision 29 of the UK Corporate Governance Code 2024 introduces new requirements for Boards to describe how they monitor the effectiveness of their internal control and risk management framework, and to provide a declaration on the effectiveness of their material controls. To prepare for our first declaration in the 2027 Annual Report, we initiated a three-year programme in 2024 to strengthen where required and align our processes across the business.

The timeline summarises the steps we have taken so far and the activities planned as we move towards full implementation.

1. Preparation phase

FY 24/25

Worked closely with key stakeholders across the business to define our approach to Provision 29 and initiate our readiness programme.

Identified the risks that the Board considers material to the business, derived from our principal risks.

FY 25/26

- Identified the material controls which support the mitigation of the material risks in scope.
- Developed expected standards for our material controls to ensure they are designed to operate effectively.
- Assessed all material controls against our expected standard, identified any specific enhancements where required and worked with all relevant stakeholders to deliver these.
- Strengthened the governance environment by updating the terms of reference for key governance forums, ensuring each forum has the right mandate, decision-making authority and cadence to provide robust risk and control oversight.
- Mapped existing assurance activities against the material controls, to ensure that the Board is comfortable with the level of assurance to support the future Board declaration.
- Developed a robust end-to-end sign-off process with material control owners and simulated the roll up for the Board declaration process, further embedding alignment to the Code ahead of full implementation.
- Regular updates provided to the Audit Committee and the Board to support effective oversight and feedback on the proposed approach.

2. Reporting phase

FY 26/27

Full implementation of the new requirements under Provision 29. The Board to carry out a review of the effectiveness of the Group's risk management and internal control framework. Our first declaration on the effectiveness of our material controls will be included as part of the 2027 Annual Report.

Internal financial controls

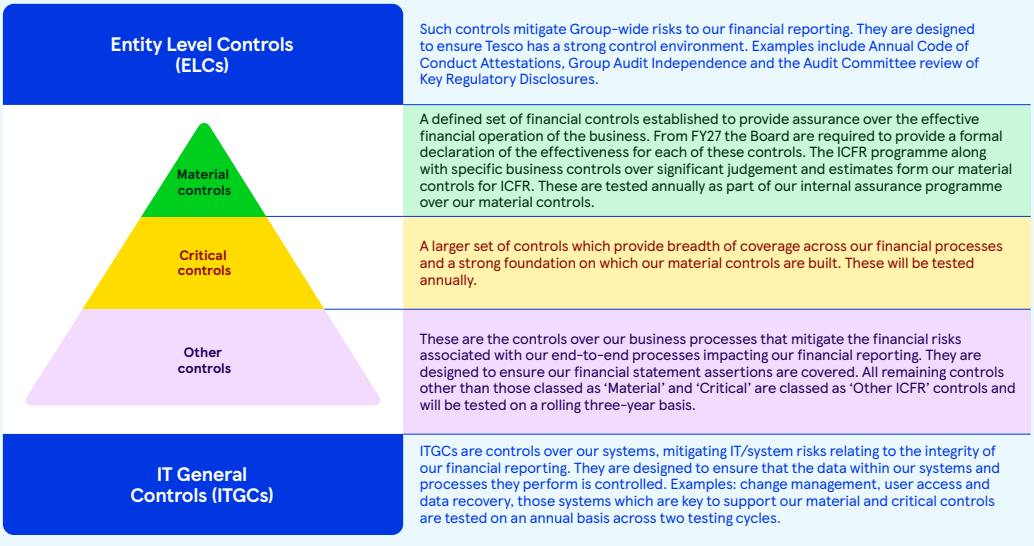
During the year, on behalf of the Board, the Committee conducted a review of the effectiveness of management's internal financial controls framework. The Committee did this principally through updates provided to it by management, Group Controls and Compliance, Group Audit, and the external auditor. Management is responsible for identifying and managing financial risks, and for maintaining an effective internal financial controls framework that identifies financial risks, maps these to controls and gives assurance over the effective operation of its control activities.

Throughout the year, work continued to embed the Internal Controls over Financial Reporting (ICFR) programme as a business-as-usual activity, and the Committee received regular updates from the Group Financial Controller on the progress of the ICFR programme, including the progress made within TBS, IT General Controls and IT automated business process controls.

Management operates a three lines of defence model, including financial controls testing by the Group Controls and Compliance team which is independent of the relevant control operators and use of the Group Audit function as a third line of defence. Such testing includes validation of IT general controls, IT automated controls as well as manual business process control activities, and entity level controls.

The ICFR programme will support the Provision 29 Code assurance statement in FY27.

The ICFR Framework



Did you know:

Significant progress has been made over the last two years in improving and enhancing the Tesco IT general control environment, facilitating greater reliance on automated controls within our ICFR framework, and enhanced reliance on our control environment by our external auditor.

Source: 2026 Tesco ARA

Example 5

Wickes 2025 ARA, p. 75, 99

Provision 29 of the UK Corporate Governance Code

Business readiness activities relating to changes brought by the Code, specifically the approach and roadmap to achieve compliance with the amended Provision 29, has been a key focus for the Board in 2025. Initial phases included reviewing the current risk and controls framework, mobilising a new controls team and sourcing a new Governance, Risk and Compliance system.

As a result of the work undertaken during the year, the business has defined and documented 30 material risks and 36 material controls to mitigate the Company's principal risks. Material control performance is being recorded and control owners have started to formally record their assessment of the design and operational effectiveness of their controls. Management provided the Board with activity updates throughout the year.

Key activities undertaken in 2025

February 2025	March 2025	April 2025	December 2025	December 2025
Definition of materiality	**Identification of material risks**	**Implementation of Governance, Risk and Compliance solution**	**Documentation of material controls**	**Launch of first line assurance activities**
Materiality was defined for the four risk categories: strategic and financial, operational, financial/non-financial reporting and compliance.	Material risks were identified from the Group Risk Register and were directly linked to our principal risks.	A third party solution was implemented during the year to evidence and monitor the operation of material controls.	Material controls were identified and documented across the business.	Control owners and performers started to record the performance of their controls and perform regular self-assessments.

The Committee's focus during the year has been on the work undertaken to identify and document material controls and to monitor the development of material controls across the business. The Committee has received assurance from management that these controls are appropriately documented and that the expected control activities are taking place. Whilst the robustness and resilience of material controls continues to improve, there remains a high level of reliance on manual detection controls. The Company's strategic transformation programme will optimise and automate a significant proportion of these manual controls, further strengthening the control environment.

The Committee also received reports on the implementation of a Governance, Risk & Compliance system. During the year, the system was fully implemented and is now being used to evidence and monitor the operation of material controls, supporting the existing assurance mechanisms that are in place.

At the year end, the Committee reviewed the effectiveness of the risk management and internal control systems, including all material controls. Noting the improvements made in 2025 and taking into account the manual detection controls in place, the Committee concluded that the internal control environment was effective.

The Committee recognises the importance of continuous improvement in the effectiveness of the Company's systems and processes, and is highly focused on ensuring that the Company delivers the required improvements to its material controls, as well as addressing the requirements of Provision 29 of the UK Corporate Governance Code 2024.

Source: 2025 Wickes ARA

Example 6

Breedon 2025 ARA, p. 59

Preparing for Provision 29

Throughout 2025 we have been preparing for the implementation of the amended Provision 29 of the 2024 UK Corporate Governance Code. Provision 29 concerns risk management and internal controls, with the first Board declaration in relation to the effectiveness of the Group's material internal controls in respect of financial, reporting, operational and compliance risks required in the 2026 Annual Report.

1 Approach to identification of material controls

Our second-line Group Risk and Controls team have led the process reviewing the Group's risk profile, utilising the existing risk management and internal control frameworks, to determine those that are a 'material' risk, to the Group.

For each material risk we have identified the most critical controls, which are relied upon by senior management and the Board to oversee and manage the risk.

2 Scope

We identified 31 material controls across our identified risk areas: financial, reporting, operational and compliance. Cyber, IT and legal compliance controls formed part of this review as well as entity level controls, such as delegation of authority and whistleblowing.

We have been able to leverage the work undertaken to evolve the Group's approach to risk and control over recent years to rely on higher level frameworks, such as the Group's financial controls framework, to reduce the number of individual controls.

3 Board engagement and embedded accountability

The Audit & Risk Committee, on behalf of the Board, has been actively involved in the scoping process to support alignment between executive and non-executive management, and the outputs from the process have been subject to review by RSM, our outsourced internal auditor.

Each material control has been assigned a named senior manager who is responsible for the ongoing effectiveness of the control and accountable to the Board.

4 Assurance planning

The Group Risk and Controls team have undertaken preliminary testing, including design and implementation walkthroughs, to understand the baseline and establish what effectiveness looks like for each control. Where gaps were identified, improvement plans were put in place.

Our assurance policy and five-year plans have been updated to incorporate specific requirements in respect of the material controls identified, which are as follows:

- Annual attestation of effectiveness from each process owner;
- Annual internal testing by the Group Risk and Controls team of each material control; and
- Third-line testing, either through RSM's internal audit or another appropriate third-party, of a selection of controls on a rotational basis.

Source: 2025 Breedon ARA

Example 7

Inchcape 2025 ARA, p. 68-69

Provision 29
As noted last year, the Committee has monitored the activities to achieve compliance with Provision 29 of the UK Corporate Governance Code 2024 which is effective from 1 January 2026. The Internal Controls team presented an update of progress against the plan at each meeting with key milestones being agreed by the Committee throughout the year.

An ad hoc Committee meeting was held in November to focus and agree on the definition of 'material controls' and readiness of the organisation for 2026 implementation. To assist the Committee in assessing the proposed material controls framework, cyber controls were selected as a pilot project during the year. This enabled the Committee to carry out a 'deep dive' into the proposed processes and to consider the resulting outcomes. The project also included benchmarking, provided an overview of effectiveness and monitoring measures to be provided to the Board, and the drafts of proposed declarations and supporting narratives.

Please see page **69** for our case study which sets out the work undertaken during the year by the Committee and the plan for 2026.

Plans for 2026

The Committee will monitor the self-certifications provided as part of the ICS framework assessing the effectiveness of the controls, reviewing supporting evidence tested through a control's certification programme delivered by a mix of second and third lines of defence.

Powered by strong governance

Overview of preparation for Provision 29 implementation

A two-year readiness journey was undertaken to ensure the Group is fully aligned to comply with Provision 29 of the UK Corporate Governance Code 2024. The Committee assessed the approach taken by management which focused on the controls which are most important in mitigating key risks that threaten the long-term sustainability of the business and where these fail, may influence decisions made by the users of the information.

The Committee:

- considered and approved the definition of material controls and are satisfied that these have been correctly identified and are material to the business;
- approved the embedding of the material controls within the existing InControl Standards (ICS) framework which is well understood by colleagues across the Group;
- provided oversight of the assurance mapping and for the pilot held in the year, monitoring outcomes and effectiveness; and
- approved the ICS training programme developed to further embed the material controls ensuring colleagues have a clear understanding of the part they play in leading a controls and compliance culture.

Plans for 2026

The Committee will monitor the self-certifications provided as part of the ICS framework assessing the effectiveness of the controls, reviewing supporting evidence tested through a control's certification programme delivered by a mix of second and third lines of defence.

Source: 2025 Inchcape ARA

Example 8

Pearson 2025 ARA, p. 110

The Committee reviewed the detail underpinning these factors as part of the 2025 year-end process. The Committee also reviewed all internal financial control deficiencies identified during the year and noted that the majority were remediated during 2025. The impact of any unremediated deficiencies on the financial statements was considered. Following these reviews, the Committee confirmed that Pearson's risk management and internal control framework operated satisfactorily throughout the year.

The Board is ultimately accountable for effective risk management in Pearson and determines our strategic approach to risk. It confirms our enterprise risk management framework as well as our risk appetite targets. The involvement of the Board and Committee in the design, implementation, identification, monitoring and review of risks (including setting risk appetite and reviewing how risk is being embedded in our culture) is outlined in more detail in the Risk management section on page 56.

Preparing for revised Code Provision 29

Following the publication of the revised UK Corporate Governance Code in January 2024, and throughout 2025, the Committee has closely overseen management's response to the new requirements of Code Provision 29. This provision will require the Board to make an explicit declaration on the effectiveness of material controls as at the balance sheet date, beginning with the 2026 financial year.

The Committee has been attentive to Pearson's proposals to address the new Code requirements, with specific focus on: (i) the identification of 'material controls' including financial, operational, reporting and compliance controls; and (ii) the assurance that is in place to provide sufficient comfort to the Board in making the required declaration.

As part of this work, we have challenged ourselves to concentrate on the controls that truly impact Pearson's success or failure, in line with the FRC's guidance.

A management working group including representatives from Internal Audit, Risk Management and Company Secretariat, and sponsored by the Chief Financial Officer, has led Pearson's preparations for the revised Provision 29. The Committee – which has led the oversight of Provision 29 readiness on the Board's behalf – has regularly reviewed management's proposals, provided input, challenged assumptions, and ensured that management's proposed approach aligns with the aims of the new Code.

In late 2025, the Committee reviewed the final proposals from management in respect of material controls and the assurance framework and recommended to the Board that the proposals be endorsed for use throughout 2026. The Board confirmed its endorsement of the approach. You can read more detail in the sections below on our agreed approach.

In 2026, the Committee's attention will shift to the review and oversight of the identified material controls, consideration of any areas of ineffectiveness or potential improvement, and preparation for future external reporting requirements.

Identification of material controls

A key responsibility under Provision 29 is for the Board to determine which internal controls it considers 'material' to Pearson – that is, those controls most critical to the long-term sustainability of the company. In order to identify the material controls, Pearson undertook a risk-based control mapping exercise. This process included:

- Mapping Pearson's principal risks and corresponding mitigating actions to their related control and governance activities
- Formally documenting existing activities as controls and confirming control owners
- Linking controls to the established SOX framework where relevant
- Incorporating feedback from external advisers and peer discussions to benchmark our approach
- Refining the controls based on an assessment of materiality

The resulting material controls span our seven principal risk categories, business units and Group-wide functions and take account of the examples provided in the FRC's guidance.

You can read more about our principal risks and mitigating actions starting on page 57.

Assurance framework and pilot programme

A robust assurance framework has been established to support the Board's future declaration of controls effectiveness.

The assurance approach includes:

- Cyclical testing by Internal Audit to ensure 100% coverage of material controls over a two-year cycle, with annual testing prioritised for higher-risk controls, those with lower existing levels of first or second line assurance, or those where Pearson has a lower risk tolerance
- Annual management self-assessments and attestations, reviewed by Internal Audit, to ensure completeness and rigour

- Reliance on SOX testing and existing external assurance where appropriate, to avoid duplication
- Regular updates on control status and operation to the Board and its Committees through a range of risk deep-dive sessions, which will ensure Board-level attention on every material control at least annually
- Interim and final assurance reports to the Board and Audit Committee each year on material controls status

The Committee has concluded that this framework is appropriate as it balances risk, independence and efficiency, and will ensure that the Board receives reliable assurance over the controls most vital to Pearson's success. The Committee recommended the framework to the Board, which accepted this recommendation.

In the second half of 2025, the Internal Audit team commenced a pilot assurance programme to test the design and effectiveness of 80% of the material controls. This pilot programme enabled:

- Control owners to be familiarised with the requirements of the new framework, including control walkthroughs with Internal Audit
- Evaluation of controls to ensure they met internal materiality criteria
- Identification of any areas for improvement in existing control activity ahead of implementation
- Opportunity to design, implement and calibrate the assurance and testing approach, reporting and tools
- Assessment of resourcing impact for employees involved in the process

In February 2026, alongside its consideration of the Provision 29 assessment for the 2025 financial year, the Board and Committee reviewed the results of the pilot assurance programme including the effectiveness status of the selected pilot controls.

Internal training and readiness

To prepare for the new requirements, comprehensive communications and training were rolled out to all control owners and Pearson Executive Management sponsors, led by the Internal Audit team.

Internal Audit are providing ongoing support and guidance to control owners as we move into the first full year of compliance with the revised Provision 29.

Source: 2025 Pearson ARA

Example 9

Howden Joinery 2025 ARA, p. 132

Case study

Provision 29 readiness and material 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 three-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.

The Audit Committee anticipates that it will report in full against Provision 29 in the 2026 Annual Report and Accounts.

Source: 2025 Howden Joinery ARA

Example 10

Molten Ventures FY26 ARA, p. 66, 76, 101

External review

The Group commissions quarterly compliance monitoring reports from IQ-EQ. Langham Hall UK Depositary LLP continues to provide depositary services for the Company and Molten Ventures' Irish Co-Invest vehicle, including asset safekeeping, oversight, and reporting. Representatives of the Depositary attended a meeting of the ARVC following financial year end to report on activity completed and any associated recommendations, with no items identified as being high risk or in need of remedial action.

Whistleblowing

The Group operates an established Whistleblowing Policy which allows employees to confidentially raise concerns regarding any suspected impropriety, including in the areas of financial reporting, controls, or other risk management issues. This policy applies to all Molten Ventures personnel and is reinforced through periodic training to ensure awareness and understanding.

Material controls framework and Provision 29

A significant governance development during FY26 has been the Group's preparation for the new internal controls reporting requirements under Provision 29 of the 2024 UK Corporate Governance Code ("Provision 29"). Provision 29 requires boards to make a declaration on the effectiveness of their material internal controls, and will first apply to the Company for accounting periods beginning 1 April 2026, meaning the first required disclosure is due to appear in the FY27 Annual Report.

During FY26, the Board, through the ARVC, has overseen the development of a comprehensive Material Controls Framework, which identifies and maps 40 material controls across the Group, organised into four primary categories aligned with the 2024 Code:

- Financial Controls (9 controls) — covering financial reporting, treasury management, tax compliance, and accounting integrity, including budget preparation and approval, management accounts production, cash flow forecasting, bank reconciliations and payment controls, FX risk management, treasury and debt covenant compliance, group consolidation, IFRS compliance, and tax planning;
- Operational Controls (10 controls) — covering investment decision-making, investment valuations, portfolio monitoring, investment AML/KYC, due diligence, IT systems and cybersecurity, business continuity and disaster recovery, third-party service provider oversight, data protection and UK GDPR compliance, fund administration, and ERP system integrity;
- Reporting Controls (10 controls) — covering annual report production, interim results, RIS and market announcements, sustainability reporting, risk disclosure, viability statement, corporate governance disclosures, directors' remuneration reporting, financial promotions, and prudential regulatory reporting; and
- Compliance Controls (11 controls) — covering FCA regulatory compliance (AIFMD), SM&CR and fitness and propriety, conflicts of interest management, market abuse prevention, anti-bribery and corruption, whistleblowing, workforce competence and compliance awareness, modern slavery and human rights, board and committee effectiveness, client money and asset safeguarding, and investor AML/KYC.

The framework applies a proportionate, risk-based approach to control classification, recognising four control types: Elevated Key Controls (individual process-level controls requiring granular oversight); Cluster Controls (groupings of related controls addressing a specific risk); Entity-Level Controls (organisation-wide pervasive controls); and Single-Risk Frameworks (specialised frameworks for specific principal risks, such as the Investment Valuation Process and the FCA Regulatory Compliance framework).

The ARVC has reviewed and considered the framework in detail during FY26. The Committee confirmed that no member had any concern that the Company's internal control environment was inadequate or that control failures were going unidentified or unaddressed. The framework is targeted for substantial completion during summer 2026, with the Board's Provision 29 declaration to be made in the FY27 Annual Report. Further detail on the Committee's oversight due of this work is set out in the Audit, Risk and Valuations Committee Report on page 99.

Risk framework updates in FY26

The following enhancements to the risk governance framework were made during FY26:

- Risk management platform — the Molten Ventures Corporate Risk Register was fully migrated onto a specialist third party platform during the year, enabling more dynamic, real-time risk monitoring and reporting, and supporting the tracking of risk ownership, mitigation actions, and control effectiveness in line with the enhanced expectations of Provision 29;
- Updated terms of reference — the ARVC's terms of reference were updated to reflect the requirements of the 2024 UK Corporate Governance Code, including the Committee's oversight role in relation to material internal controls, and to clarify the distinction between the Committee's governance responsibilities and the regulatory responsibilities of the Alternative Investment Fund Manager (AIFM);
- Revised Group Valuation Policy — the Group Valuation Policy was updated in response to the FCA's Private Market Valuations Review feedback and revised IPEV guidelines, including the introduction of a formal ad hoc revaluation process and updated scenario-based OPM methodology; and
- Financial Position and Prospects Procedures ("FPPP") — the FPPP was updated following its annual review, providing the ARVC with assurance over the internal controls and associated processes in place at the Company.
- New compliance platform — A new internally developed compliance platform was adopted for tracking notification and approval flows, bi-annual attestations, and annual fitness and propriety assessments.
- Internal development of a new Material Controls Framework as described above.

8. Financial reporting integrity

Accurate, complete, and compliant financial and non-financial reporting

Link to KPIs
1, 2, 3, 5

NEW PRINCIPAL RISK –

This risk has been separated out from the Group's broader compliance risk in FY26 to more clearly delineate financial reporting integrity as a discrete risk category, in line with the way the 2024 UK Corporate Governance Code distinguishes between compliance and reporting risks. The Group's underlying controls framework is unchanged; the work undertaken in the year has been directed at supporting the new Provision 29 internal controls declaration.

Potential impact

- Material misstatement in the financial statements, whether through error or fraud, could result in restatement, regulatory action, reputational damage, and loss of investor confidence
- Failure to produce timely, accurate, and compliant interim and annual reports could result in regulatory sanction and adverse market reaction
- Inaccurate or misleading market announcements could result in regulatory action under UK MAR and reputational damage
- Failure to maintain effective controls over the valuation of unlisted investments — the most significant area of judgement in the financial statements — could result in material misstatement
- Inadequate controls over non-financial reporting (including sustainability disclosures) could result in regulatory action and reputational damage
- Failure to make a compliant Provision 29 declaration in the FY27 Annual Report could result in adverse regulatory and investor action

Risk management and mitigation

- Multi-stage review process for annual and interim reports, with Board and ARVC approval
- Investment Valuation Process governed by a single valuation policy, ring-fenced from the investment team, incorporating a four-eyes review and ARVC oversight
- Management reporting prepared monthly with a three-step review process;
- Dual authorisation required for all material payments; bank reconciliations completed within two working days
- CFO/Company Secretary sign-off process for all RIS announcements, with legal and compliance review for material announcements
- Annual review of accounting policies; external tax adviser oversight with documented review and approval processes
- Fund Controller review and approval of all fund administration packs prior to release or use for financial reporting

Changes/activities during the year

- Material Controls Framework developed during FY26, identifying 40 material controls across four categories (Financial, Operational, Reporting, and Compliance), aligned to the 2024 UK Corporate Governance Code Provision 29
- ARVC confirmed satisfaction with the internal control environment and endorsed the Company's approach to Provision 29 preparation at its March 2026 meeting
- FRC's revised Provision 29 guidance published during the year, confirming a more flexible, proportionate, and principles-based approach; first application for the Company is for accounting periods beginning 1 April 2026
- Updated Group Valuation Policy approved, incorporating revised IPEV guidelines and FCA PMVR feedback
- Adoption of an updated Financial Crime Risk Assessment to include qualitative narratives and quantitative scoring following FCA industry feedback on best practices.
- Risk management platform fully operational, supporting real-time risk monitoring and control effectiveness tracking
- PwC audit for FY26 completed with no material misstatements identified. Improved collaboration and process efficiency noted

Focus for FY27

- Finalisation of the Material Controls Framework and preparation of the Board's first Provision 29 declaration for the FY27 Annual Report
- Monitoring of first-wave Provision 29 disclosures (calendar year-end reporters) to inform the Company's own reporting approach
- Continued development of the annual effectiveness assessment process for material controls

FRC Code Provision 29 — Internal controls

A key area of focus during FY26 has been the Committee's work in preparing for the new internal controls reporting requirements under Provision 29 of the 2024 UK Corporate Governance Code ("Provision 29"), which requires Boards to make a declaration on the effectiveness of their material internal controls. Provision 29 will first apply to the Company for accounting periods beginning 1 April 2026, meaning the first required disclosure will appear in the FY27 Annual Report.

Building on the Company's already robust internal controls framework, the Committee has overseen significant work during FY26 to enhance and formalise the reporting infrastructure required under Provision 29. This included a comprehensive controls mapping exercise covering over 40 controls across multiple business areas, aligned to the Company's principal risks, which served to document and articulate the strength of controls already embedded across the business. This work was led by the Company Secretary, Finance team and legal and compliance teams, with oversight from the Committee at each of its meetings during the year. Post year end the Policies & Procedures Committee's terms of reference were approved with delegated responsibilities from the Board and other group management Boards to implement the day-to-day running and assessment of the effectiveness of the material controls to assist the Directors in making the required attestation next year.

The Committee noted the FRC's revised guidance on Provision 29, published during the year, which informed discussion of the previously anticipated scope and prescriptiveness of the reporting obligation. The revised position confirms that companies are required to provide assurance on material controls; that specific disclosure of a commercially sensitive control failure is not required; and that the overall direction of travel is towards a more flexible, proportionate and principles-based approach. The regime continues to operate on a comply-or-explain basis.

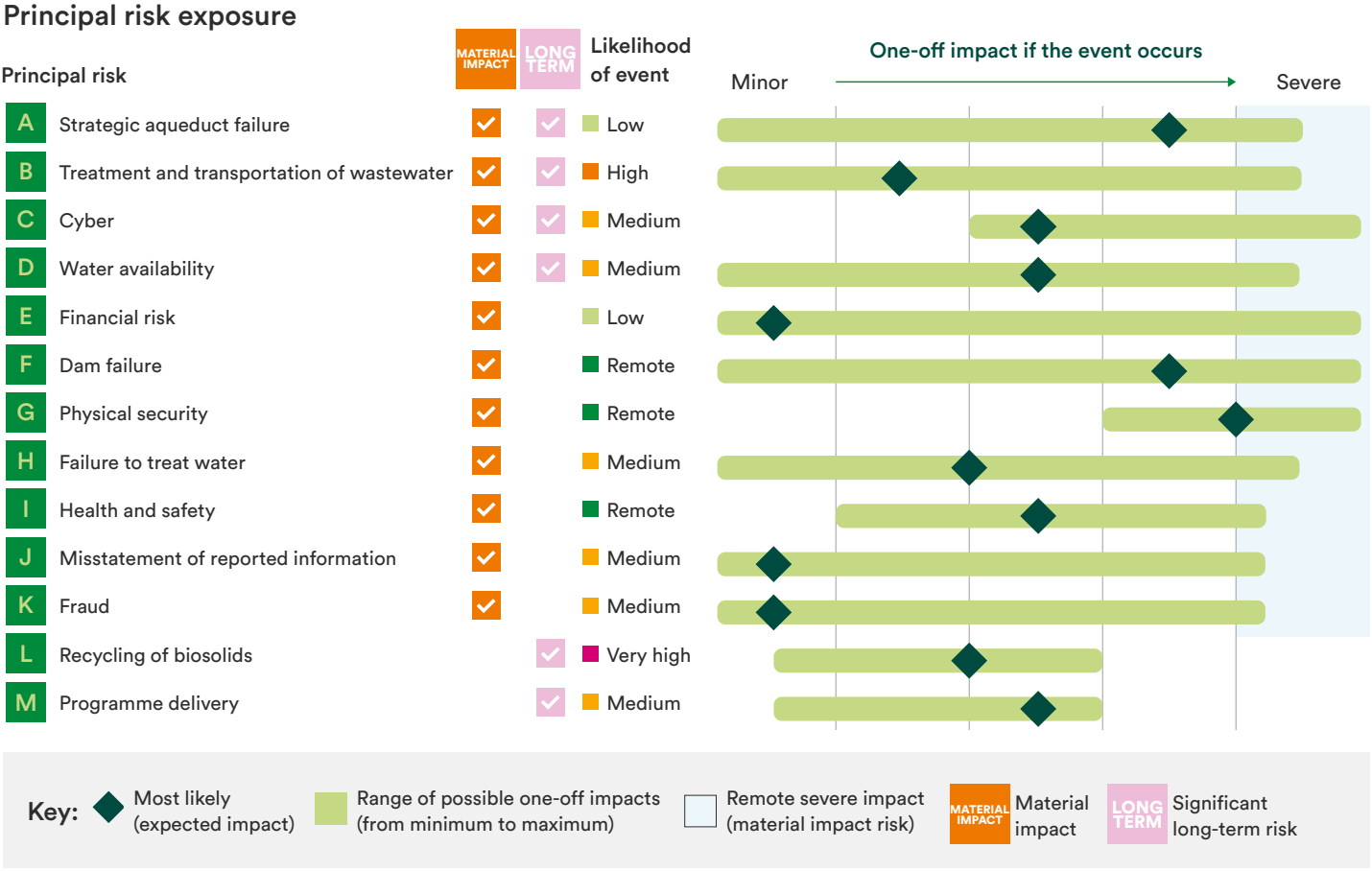
The Committee confirmed that no member had any concern that the Company's internal control environment was inadequate or that control failures were going unidentified or unaddressed. The Committee endorsed a pragmatic approach for FY26: to continue developing and documenting the internal controls framework, to monitor how disclosure expectations develop in practice among first-wave reporters (those with calendar year-end accounting periods), and to finalise the Provision 29 reporting approach in time for the FY27 Annual Report.

Source: 2026 Molten Ventures ARA

Example 11

United Utilities 2026 ARA, p. 57-58, 124, 130

Principal risk exposure



Our principal risks

Our principal risks 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 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.

A declaration of the effectiveness of material controls as required by Provision 29 of 2024 revisions of the UK Corporate Governance Code (the code), will be made in the financial year 2026/27; however, in preparation for this declaration, material controls have been listed alongside the material impact risks on pages 58 to 61, together with governance and assurance.

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 61.

The bar chart 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 shaded blue box), it is regarded as being material, constituting a material impact risk.

Over the last twelve months, ten of the thirteen principal risks have remained relatively stable from an aggregate position, with three principal risks demonstrating a movement in exposure:

- **Cyber:** The risk has increased to reflect the increasing external threat despite steps taken to strengthen our internal preventative and responsive capability.
- **Dam failure:** There has been a reduction in the aggregate likelihood of dam failure following the completion of capital investment. The overall dam risk continues to evolve as dams are subject to periodic assessment along with further capital schemes to improve dam safety.
- **Programme delivery:** The capital programme has reduced to reflect increased confidence in the deliverability of the plan following a year in which the committed rate of spend is in line with schedules.

Our principal risks

Principal risk	Risk exposure	Control/mitigation	Governance and assurance
A ↔ **Strategic aqueduct failure** MATERIAL IMPACT LONG TERM	We own and operate nine aqueducts, which transfer water from major treatment works and large service reservoirs to the wider network. Asset deterioration and damage (caused by third-party or natural events) are key risk factors to water supply and/or quality relative to large proportions of our customer base. The Haweswater Aqueduct is the most significant asset of this type and currently has the lowest level of resilience.	We are committed to delivering a resilient supply of water. Material controls are: • **Rehabilitation/restoration:** The Large Diameter Trunk Mains (LDTM) inspections regime, along with existing asset maintenance programmes, are structured and reviewed periodically to identify where major rehabilitation or restoration programmes are required. The programmes are centrally governed and delivered to ensure the successful rehabilitation and restoration of strategic aqueducts, reducing the likelihood and impact of structural failure. Current initiatives include the Haweswater Aqueduct Resilience Programme and the Vyrnwy Aqueduct Modernisation Programme. • **Aqueduct loss contingency plans:** Plans to outline response to total loss of supply (in the event of breach) or restrictions on use (in the event of a water-quality event) are developed, maintained and periodically exercised to enable the rapid deployment of resources and engagement with external agencies to maintain community function. Other controls include protective easements, inspections, and the monitoring of flow, pressure and turbidity via sensors and alarms.	**Governance** • Water quality first board[M] • Water price control[M] • Ofwat liaison committee (HARP)[M] • HARP delivery board[M] **Assurance** • Engineering team technical reviews[2] • Assurance team reviews[2] • Cyclical internal audits[3]
B ↔ **Treatment and transportation of wastewater** MATERIAL IMPACT LONG TERM CLIMATE	We own and operate network and treatment assets to collect and treat wastewater before it is safely returned to the environment. Risk factors to the hydraulic and operational capacity include: population growth; extreme weather (amplified by climate change); increased surface runoff due to residential and commercial developments; improper or harmful use of the sewer systems; and inherent asset health issues. Consequential failure, now subject to tightening legislation, can result in unpermitted storm or emergency overflow activations, sewer flooding and environmental damage.	We focus on providing reliable and resilient wastewater services. Material controls are: • **Maintenance:** Proactive and reactive inspection, servicing, repair and replacement activities are planned, prioritised and completed across wastewater assets to maintain operational reliability and reduce the likelihood of asset failure and environmental impact. • **Licence to operate:** Mandatory training, certification and competence requirements for wastewater operations are defined, delivered and routinely refreshed to ensure staff maintain the necessary skills and qualifications to safely and effectively operate the wastewater processes and assets. • **Power resilience:** Power resilience plans and assets are maintained for critical wastewater sites to ensure continuity of treatment and transportation during power interruptions and outages. Other controls include customer awareness, trade effluent management, monitoring of sensors and alarms and emergency response. In addition, our better rivers programme focuses on improving river water quality and reducing spills from storm and emergency overflow operation.	**Governance** • Wastewater price control[M] • Flood committee[M] • Pollution committee[M] **Assurance** • Assurance team reviews[2] • Cyclical internal audits[3]
C ↑ **Cyber** MATERIAL IMPACT LONG TERM	As we continue to develop our digital capability, we become more reliant on connected technology, not only in the way we operate, but also the way in which we communicate with our customers and the wider community. Cyber incidents continue to grow in all industries with a constantly changing threat landscape. The potential for data and technology assets to be compromised is a key risk to business processes and operations.	We employ a multi-layer control environment. Material controls are: • **Infrastructure access controls:** Perimeter and internal firewalls, supported by intrusion detection systems, are centrally configured, monitored and routinely updated to restrict unauthorised access and detect malicious activity across the corporate and operational technology networks. • **System access controls:** System, data and internet access is restricted through centrally managed authentication, authorisation and usage controls, ensuring users are granted only the permissions required for their role and preventing unauthorised or inappropriate access across information and operational technology (IT and OT) environments. • **Point protection:** Anti-malware suite and mail gateway service, which includes malware detection, transmission protocols, and endpoint actions. • **Monitoring and response:** The Security Operations Centre continuously monitors security events, analyses threat activity and coordinates timely incident response actions to detect, contain and mitigate cyber threats across the organisation's IT and OT environments. We also operate a comprehensive cyber security incident response plan with associated training and exercising. Other controls include security awareness training and business continuity plans.	**Governance** • Security steering group[M] • NIS governance board[M] • Group audit and risk board (GARB)[M] **Assurance** • Security team reviews[2] • Annual internal audit[3] • External reviews[3]

Key:

Risk categorisation

MATERIAL IMPACT Material impact

LONG TERM Significant long-term risk

CLIMATE Climate-related risk

Governance

M Management committee

B Board committee

Assurance (refer to pages 134 to 135)

2 Second-line assurance activity

3 Third-line assurance

Change in risk exposure over the year (see page 57 for explanation)

↔ Stable ↑ Increased ↓ Decreased

Provision 29 of the UK Corporate Governance Code: material controls declaration preparedness

The committee has closely monitored the progress of work underway to support the first 'declaration of the effectiveness of the material controls' (the material controls declaration) that will be provided at the balance sheet date of 31 March 2027 in accordance with code provision 29. Since the 2024 code was published, work has focused on providing the board with an increased level of confidence in making the material controls declaration utilising existing governance and assurance frameworks (see pages 55 and 57). Following the redefinition of our principal risks last year along with the identification of our material impact risks and material controls (see pages 57 to 61), the committee was updated on the outcome of a benchmarking exercise to gain confidence over the company's approach.

The benchmarking involved management meeting with KPMG and the Financial Reporting Council and the presentation of the approach at a session of the FTSE 100 Group for CFOs. The company's quantitative approach to identify material risks was noted as being a more scientific and mature approach compared to the alternative qualitative approach.

Material controls declaration project

Following the publication of the 2024 code, work commenced to evolve the approach to principal risks and material controls and the board's preparedness to being able to provide, with confidence, a material controls declaration as required by provision 29 of the code. The activities to date are summarised below.

2024	2025		2026
Refining and expanding our existing disclosures regarding effectiveness of risk management and internal controls	Redefined our principal risks as: • Material impact risks • Significant long-term risks	Identifying our material controls (and their governance) which mitigate our material impact risks	Improving the board's line of sight of the effective operation of material controls: • Evidencing control effectiveness • Assurance of control activities
Approved by the board and disclosed in 2024 annual report	Approved by the board and disclosed in the 2025 annual report		A 'dry run' was scheduled to be presented to the board in May 2026

During the year, the audit committee has been kept fully informed of progress of the material controls declaration project, providing feedback and suggestions to management – including that the board should have early sight of and fully understand what information would be presented to it in order to make the declaration, not only in relation to the material risks, but to show it had been engaged in reviewing the material controls over a suitable time period. The existing governance, risk management, internal control and assurance frameworks will be utilised to support the material controls declaration.

In November 2025, the board was apprised of the progress of the project – including the provision of a draft material controls reporting tracker which would summarise the material impact risks and associated material controls, a view and explanation of the effectiveness of the controls and any supporting assurance. A further deep-dive session was held with the board in February 2026, updating on progress and providing a further opportunity for discussion, obtain the views of board members and points for management to action. It was agreed that a 'dry-run' would be undertaken for the 31 March 2026 year, and was scheduled to be presented to the board in May 2026.

Source: 2026 United Utilities ARA

Example 12

Mears 2025 ARA, p. 71

Reform of UK Audit and Corporate Governance Framework

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 opposite.

An initial proposal on material controls (financial and non-financial) and assurance has been reviewed by the ARC and is subject to further enhancement in preparation for a "dry run" in Q3 2026.

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. Efforts have been focused on leveraging this strong foundation and strengthening any gaps to ensure the Board has the requisite level of confidence in making its annual declaration on the effectiveness of material controls.

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 is likely to influence decisions made by users of the information.

The Committee has been informed by looking beyond Mears' principal risks and reviewing the output of a broader assurance mapping process to ensure that other critical and emerging risks were identified and considered. In addition, risks and controls attached to financial reporting and fraud have also been tabled by the senior management team and considered by the Committee.

Key milestones to compliance	
January 2024	FRC published the UK Corporate Governance Code 2024 and supporting guidance
October 2024	Detailed review and update of principal risks
H2 2025	Internal audit plan targeted the testing of material controls attached to principal risks
December 2025	Assessment and definition of "materiality" in the context of material controls
January 2026	Workshops facilitated by Compliance Committee to identify material controls in respect of: • principal and other critical risks; • financial reporting and fraud risks; and • focused session on cyber and information security risks.
March 2026	Internal audit plan for 2026 being reviewed and updated by the Audit and Risk Committee to reflect outputs from workshops
Q2/Q3 2026	Continuation of rolling programme of principal risk material control testing
Q3	A "dry run" of material controls assurance pack to be reviewed by the Audit and Risk Committee, providing sufficient time for corrective actions to be put in place
December 2026	Annual Report for year ending 31 December 2026 to include Board's declaration on the effectiveness of material controls

Completed In progress To be completed

Source: 2025 Mears ARA

Example 13

BT FY26 ARA, p. 96, 54-55

Risk management

We want to be smart with risk. Our risk management framework gives us a simple, consistent way of looking at the challenges we face when delivering our strategy. It helps us make informed decisions that benefit our people, customers, shareholders and wider stakeholders.

Why we need our risk framework

The external risk landscape is challenging and complex. There's increasing competition, evolving market dynamics, geopolitical uncertainty, cyber security threats and risks from AI's rapid advance.

Against this backdrop, effective risk management is essential. Our risk management framework helps us identify and assess the risks we face and the best ways to manage them. It stops us taking on unacceptable levels of risk. And it also stops us unnecessarily constraining our business, or missing growth and transformation opportunities. The diagram below highlights the framework's key elements.

Risk Management Framework

GOVERNANCE – AUDIT & RISK COMMITTEE

The Board is responsible for risk management. The *Audit & Risk Committee* oversees and monitors our risk management and internal control systems' effectiveness on its behalf. Twice a year the Board receives a summary of how we're managing risks across all GRCs and Units. There are also deep dives into individual GRCs through the year. You can find more information in the **Audit & Risk Committee Chair's report** on page 91.

INPUTS

Strategy, purpose and ambition
We design our framework to help us deliver our strategy.

We use our ambition and strategic priorities as the starting point. This helps identify what might stop us from achieving them, and decide how to manage those risks and what risk level we're comfortable with.

GROUP RISK CATEGORIES

We divide our risk landscape into GRCs. Each GRC has an *Executive Committee* sponsor accountable for applying the framework to that category.

APPETITE

We define how much or how little risk we're willing to take in each of our GRCs. This lets us take opportunities as they come up without exposing ourselves to too much risk.

ENDURING RISKS

Need consistent, enduring control and assurance structures to manage them.

CONTROLS
Formal, repeatable, activities that cut the chance of an enduring risk materialising (or lessen the impact if it does).

ASSURANCE
An objective, evidence-based approach to make sure we have effective controls over key business risks.

DYNAMIC RISKS

Need bespoke treatment based on their size, impact and what we need to do about them. There are two types:

POINT RISKS
Significant to us at a point in time, can't be managed through our control framework, and need focused effort.

EMERGING RISKS
New and/or often longer-term risks, which could be materially significant, but that we can't fully define today.

OUTPUTS

Being smart with risk
Our framework embeds risk management into our day-to-day business, from top to bottom.

Being smart with risk means all of us having our personal risk radar switched on, helping everyone make better decisions.

UNITS AND PROGRAMMES

We bring together risks to review, discuss, prioritise, own, action and report on across all Units (CFUs, TUs and CUs) and programmes. This gives us insights and facilitates factual, data-driven risk conversations. Which leads to smarter risk decisions and better operational integrity.

RISK HUBS

Cross functional forums that look at risks that span multiple GRCs, for example our Sustainability and Geopolitical risk hubs.

ENABLERS

RISK EMBEDDED CULTURE

We train everyone involved with the framework to give them a strong grasp of the expectations and benefits of good risk management. We also expect our leaders to be role-models for good risk management – taking accountability, showing curiosity and providing psychological safety – and to use the framework to make informed decisions.

TOOLS AND TECHNOLOGY

We have a dedicated, integrated risk management, controls and assurance system called Artemis. It captures enduring and dynamic risks and tracks how well our control framework is working. And it manages our first, second and third line assurance activity in one place. It gives us a clear, up to date picture and is central to our reporting and monitoring at every level.

Making material risks visible to our Board

We have a consistent approach to managing risk across the group, but as our business and the wider landscape evolves, our risk management framework does too.

This year we embedded our approach for applying Provision 29 of the 2024 UK Corporate Governance Code.

This involved identifying and defining material controls with the *Audit & Risk Committee*. As a result, we've now defined the framework for each GRC as a material control. Each GRC framework includes the following risk management elements in that area:

- Governance and Oversight
- Risk Appetite
- Dynamic Risk Management
- Policies, Standards and Controls
- Assurance

We supplement these GRC framework material controls with a handful of organisation-wide controls. They include our Code of Conduct and training, the Speak Up process, our Disclosure Committee and our Delegation of Authority Framework.

This approach reflects how we manage these areas day-to-day. And it provides the Board with the highest priority risk and control information, so it knows which things need extra attention.

As part of our enhanced approach, we now prioritise underlying operational controls in each GRC to reflect the size of the risk they mitigate. This gives clearer oversight and allows assurance to be directed to the highest risk areas.

We've also kept strengthening and integrating our second line assurance activities. This helps give us the right coverage across our material controls and priority areas within our broader control framework.

Monitoring geopolitical risks

We actively monitor developments in the external environment, including evolving geopolitical conditions and their potential impacts. The situation in the Middle East is dynamic and fast-moving. In response, we have established a taskforce to monitor the threats to our business, coordinate our operational response, maintain a clear line of sight to impacts, mitigations and decision points and provide updates to the Board. Our cross-functional Geopolitical Risk Hub has also carried out longer-term scenario analysis and is assessing second- and third-order impacts. Actions are agreed and implemented as needed.

Risk management and internal controls systems

The risk, control and assurance framework has continued to be developed to enable the group to be smart with risk and make well-informed decisions. The Committee has overseen ongoing enhancements and simplification of the risk management framework – see pages 54 to 62.

The framework divides the risk landscape into dynamic risks and enduring risks which are managed through 13 GRCs covering strategic, financial reporting, operational and compliance risks. The Board monitored the effectiveness of the group's risk management and internal controls through reviews of the GRCs throughout the year. Discussion of the GRCs is split between the Board and this Committee, and I report any key matters from the Committee reviews to the Board.

Each GRC is owned by an *Executive Committee* member who attends the relevant Board or Committee meeting to discuss the status of risk and controls within their GRC. The Board or Committee robustly assessed both current, specific concerns (point risks) and uncertainties that may materialise in the future (emerging risks). The Board or Committee agreed with management any actions required to manage or mitigate these risks effectively. These discussions also include a consideration of risk appetite, the effectiveness of the controls and other mitigation activities, remediation plans and any further areas for improvement.

Each of the GRCs was discussed throughout the year, with a focus on resilience, potential reputational risk and priority areas for the business to address in order to mitigate risk, including updating legacy systems and continuing to engage with Government on key matters.

These activities enable the Committee to confirm that the group's systems of risk management and internal controls have been appropriately reviewed. Where considered necessary, targeted improvements have been planned or agreed in order to continue to transform the control environment and appropriately manage risk.

Throughout the year the Committee also considered the effectiveness of the internal controls systems and preparations underway to report in line with the updated Provision 29 of the Code from FY27. The agreed approach to material controls reflects our well-established framework and will support the Committee in focusing on the highest risk areas of the control framework where additional attention may be required. See page 55 for more information on the planned approach to material controls and reporting against Provision 29.

Source: 2026 BT ARA

Example 14

Hunting 2025 ARA, p. 96-97

Control environment and compliance with UK Corporate Governance Code (Provision 29)

Hunting's control environment is designed to safeguard assets, ensure accurate and reliable reporting, and support the delivery of strategic objectives.

The Board maintains overall responsibility for monitoring and reviewing the effectiveness of risk management and internal controls, with regular oversight by the Audit and Risk Committee.

Work completed in 2025 – Provision 29 readiness

During 2025, the Group strengthened its governance framework in line with the UK Corporate Governance Code, in respect of the new requirements of Provision 29.

Hunting's framework anchors material controls to principal risks, integrates bottom-up business unit registers with a Group level assessment, and uses AuditBoard to capture evidence, testing, and action tracking.

Throughout the year, Hunting enhanced its assurance model by formalising the three lines of defence and establishing the Internal Control Committee. This committee met to review material controls, monitor remediation progress, assess reporting quality, and set the cadence for assurance activities in 2026.

The introduction of the Risk Universe provided baseline registers across segments, enabling consistent risk assessment and comparability.

Material controls were refined into a clearly defined set, aligned to principal risks and mapped to the Group Manual, with completeness validated against external benchmarks.

The annual financial controls self-assessment, now fully integrated into AuditBoard, confirmed the strength and reliability of the Group's control environment.

Internal Audit complemented this by completing design and effectiveness reviews in priority locations, supporting investigations, and initiating independent testing of material controls to underpin compliance with Provision 29.

Deloitte updated the full-year 2025 audit plan, reviewed the approach to material controls and control reliance, completed component visits and provided interim feedback on D365 implementations, revenue recognition, inventory valuation, management override of safeguards, and restructuring disclosures.

Planned and agreed actions for 2026

Looking ahead to 2026, the Board approved a balanced assurance approach with twice-yearly reporting to the Audit and Risk Committee.

Second-line design and effectiveness testing of material and key financial controls, governance controls and IT general controls will be completed by mid-year and year-end, with independent testing of material controls reported in February and August.

Material controls will be refreshed and presented for approval in April, incorporating risk movements and lessons learned. Non-financial information assurance will continue in 2026 and consideration given to expanding the scope of work to include a broader set of metrics.

Technology enablement will deepen as D365 Phase 2 standardises configuration and workflows, strengthening segregation of duties and automated controls, while AuditBoard provides real-time evidence, grading and close-out tracking for findings.

Enhanced scenario testing will be applied to financial reporting cut-off, project accounting, supplier master change controls, inventory valuation, cyber event recovery and data integrity, and climate-related operational resilience, with results reported through the Internal Controls Committee and Audit and Risk Committee.

The 2026 year-end process will culminate in a Board-level assessment and a clear declaration on the effectiveness of material controls at the balance sheet date, aligned with Provision 29.

Three lines of defence ("TLoD") and reporting

The TLoD remain central to this model: operational management owns risks and controls; Group Finance, QAHSE and other functions monitor, test, design and coordinate assurance; and Internal Audit provides independent reviews.

The Internal Controls Committee oversees this structure and reports outcomes to the Audit and Risk Committee and the Board.

Internal Controls Committee

The Internal Controls Committee, a sub-committee of the Executive Committee, was established in 2025. Two meetings have been held during the year to review material controls, remediation actions, and compliance with the assurance model. Reporting lines have been established to the Audit and Risk Committee for oversight.

Overview of material controls

Hunting's control environment is underpinned by a clearly defined suite of material controls, designed to provide reasonable assurance over governance, financial reporting integrity, operational resilience, and compliance processes.

These controls are mapped to the Group's Principal Risks and embedded within the Group Manual, ensuring accountability, consistency, and transparency across all operations.

Identification and scope

In 2025, Hunting completed a comprehensive review of its control framework to prepare for compliance with Provision 29 of the UK Corporate Governance Code. This review identified 46 material controls, comprising:

- 34 Entity Level Controls ("ELCs"); and
- 12 Internal Controls over Financial Reporting ("ICFR")

These controls address the most significant risks facing the Group, including strategic, operational, legal and compliance, financial reporting, fraud, and IT resilience risks.

The scope reflects external benchmarks and peer analysis to ensure completeness and relevance.

Key features of the material controls framework

Entity-level controls ("ELCs"):
Include governance and oversight mechanisms such as Board-approved delegations of authority, M&A and investment policies, a whistleblowing programme, and annual assurance statements.

These controls ensure strategic decisions, risk management, and compliance activities are executed within defined parameters and reported to the Internal Controls Committee and the Audit and Risk Committee.

Financial reporting controls ("ICFR"):
Controls over inventory valuation and existence, revenue cut-off, revenue recognition under IFRS 15, and journal entry approval processes mitigate risks of material misstatement.

These controls are supported by automated workflows within the Group's ERP system (D365) and monitored through AuditBoard for real-time evidence capture and remediation tracking.

IT general controls:
Cyber security monitoring, disaster recovery planning, and segregation of duties within core systems form part of the Material Control set, reflecting the Group's very low risk appetite for IT and cyber threats.

Non-financial controls:
Initial scope includes health and safety and product quality metrics. Future reviews will consider whether to expand the scope of metrics covered for 2027.

Assurance and testing

Hunting PLC applies the TLoD and assurance model as part of its internal control and assurance framework, which is aligned with the UK Corporate Governance Code and Provision 29 requirements.

The following outlines how the TLoD and assurance model work:

First line of defence
– operational management

Role: Business units own and operate controls day-to-day.

Key activities:
Completion of operational assurance statements at half-year and year-end to confirm entity-level controls are functioning.

Annual self-assessment of internal controls over financial reporting ("ICFR") via AuditBoard.

Direct responsibility for designing, implementing and evidencing controls linked to principal risks, including financial, operational, legal and compliance, and fraud risks.

Second line of defence
– oversight and monitoring

Role: Group finance risk and controls team provides independent monitoring and testing.

Key activities:
Design and effectiveness testing of material and key controls (financial and non-financial).

Design and monitoring of entity-level controls and reporting to the Internal Controls Committee and the Audit and Risk Committee.

Use of AuditBoard for real-time tracking of remediation actions.

Includes internal IT specialists for general IT controls ("GITC") and ERP configuration reviews.

Third line of defence
– independent assurance

Role: Internal Audit delivers independent assurance to the Audit and Risk Committee.

Key activities:
- Testing of material controls and operational effectiveness.
- Process mapping and control documentation for high-risk units.
- Fraud investigations and compliance reviews.
- Support from external specialists for IT general controls and other technical areas.

Assurance model

Role: The assurance model is structured around these three lines, with clear accountability:

- Board and Audit and Risk Committee maintain overall oversight.
- Independent assurance combines internal audit and second-line reviews, supplemented by external IT specialists where needed.
- Testing of material controls is progressing, with full effectiveness reporting scheduled to be resolved during 2026.

Source: 2025 Hunting ARA

Example 15

JTC 2025 ARA, p. 60

Principal risks and material controls

The Group continually reviews its risk taxonomy to ensure it remains complete, relevant and appropriately aligned to the Group's assessment of principal risks.

A principal risk is defined as a risk, or combination of risks, that could have a material adverse effect on the Group's business model, performance, future prospects or reputation. This includes risks that could threaten the Group's operational resilience, financial position, solvency or liquidity.

During 2025, the Board determined that no changes were required to the Group's assessment of its principal risks.

The Group maintains a comprehensive control environment and undertakes a range of measures to monitor and manage risks arising from its business activities. These measures are designed to promote ongoing awareness of key risks, controls and regulatory requirements across the organisation.

Material controls and mitigation measures include:

- A well-established acquisition due diligence framework
- A Group Compliance Framework, including a dedicated compliance monitoring function
- A Business Risk Assessment Framework to support the identification and assessment of financial crime and other enterprise risks
- A clearly articulated and consistently applied Risk Appetite Framework
- Employee training programmes designed to promote risk awareness and professional conduct
- Segregation of duties for transaction processing, including a rigorous six-eyes Recommendation for Signing approval process
- Proactive fraud prevention measures, including strengthened authentication and identity verification controls
- Performance scorecards that drive commercial performance while remaining balanced against people and risk management considerations
- Mature cybersecurity capabilities, including preventative controls, staff training and periodic testing
- Robust IT infrastructure supported by regularly tested business continuity and disaster recovery arrangements
- Rigorous employee screening and on-boarding processes
- Established talent development programmes that support employee engagement and retention
- Comprehensive induction and ongoing training for all employees
- Annual employee confirmations of compliance with core Group policies and procedures
- Whistleblowing arrangements to support the reporting of concerns
- A defined Group Risk Escalation Framework to ensure timely identification and consideration of risk events

Notwithstanding the expected delisting of the Group during 2026, the Board expects to maintain the discipline of assessing material control effectiveness in a manner consistent with the principles contemplated by Provision 29 of the UK Corporate Governance Code.

The Group also maintains insurance cover in excess of regulatory minimum requirements, providing an additional layer of protection in support of the overall control environment.

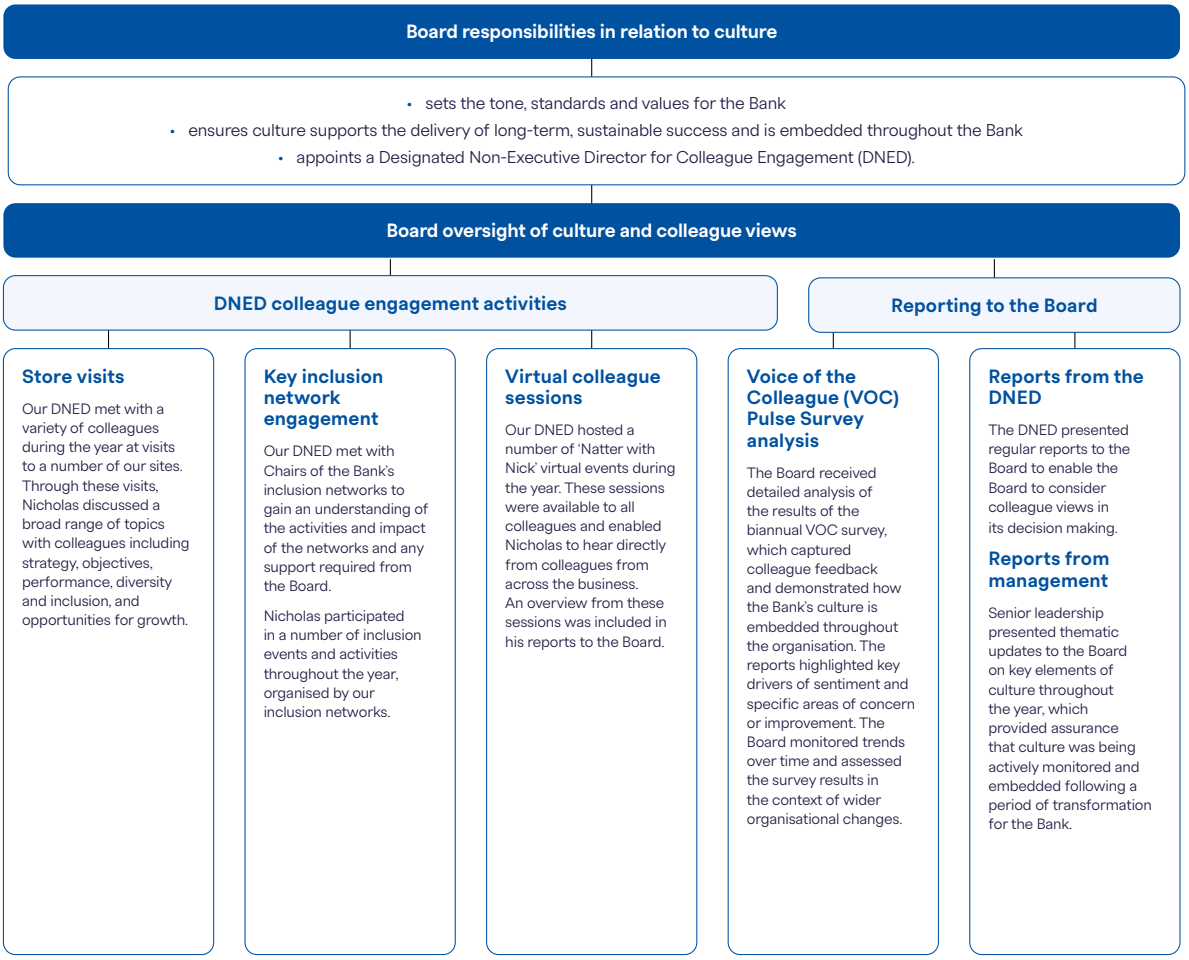
Source: 2025 JTC ARA

Example 16

Metro Bank 2025 ARA, p. 61

Board oversight of culture and colleague engagement

Our colleagues deliver superior service and are the heart of our relationship banking approach. The Board recognises the importance of our colleagues and our unique culture, and an overview of the Board's oversight is summarised below.



Designated Non-Executive Director for Colleague Engagement (DNED)

With regard to Provision 5 of the Code, we continue to be of the opinion that appointing a DNED is the most appropriate engagement mechanism for the Bank to ensure there is effective two-way dialogue with colleagues. The DNED's role is to connect colleagues with the Board and escalate their views to support informed decision making.

A note from our DNED

It was a pleasure to continue in my role as DNED for another year and engage with colleagues as they executed our strategy and delivered strong results.

I was able to meet many colleagues during the year, from a range of business areas, and their views and experience gave valuable insights which were considered in Board decision making.

The Board is committed to ensuring our culture remains something to be proud of and it was great to see our culture in action during my visits and on Viva Engage (our internal social media channel).

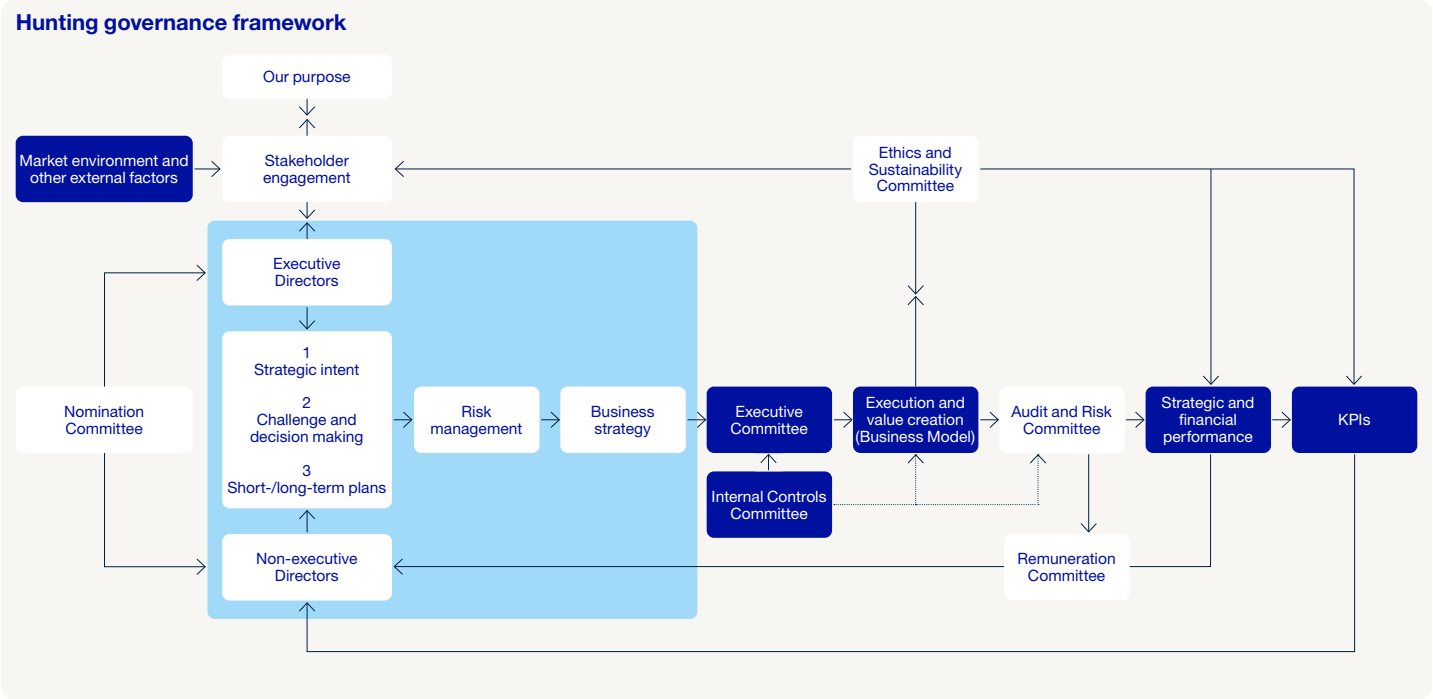
As we continue to build a bank for the future, colleagues remain at the heart of our relationship banking approach, and I look forward to meeting more colleagues and hearing their views in 2026 before handing over to my successor when I step down from the Board at the end of May 2026.

Nicholas Winsor
Designated Non-Executive Director for Colleague Engagement

Source: 2025 Metro Bank ARA

Example 17

Hunting 2025 ARA, p. 110



Source: 2025 Hunting ARA

Example 18

Standard Chartered 2025 ARA, p. 174-175

Action and decision	Outcome and impact
Internal Controls	
• Discussed reports from Group Internal Audit & Investigations covering the appraisal of controls across key risks within the Committee's scope. • In conjunction with the Audit Committee, reviewed the outcomes of the annual Risk and Control Self-Assessment (RCSA). • Reviewed and discussed an addition to its terms of reference on the oversight of material controls alongside the Audit Committee, which was recommended to the Board for approval.	• Encouraged management to ensure that the RCSA process continues to identify the real risks faced by the Group in its day-to-day operations. • Ensured that appropriate mitigations and controls are in place for material risk events.

Audit Committee report

Governance

Action and decision	Outcome and impact
Terms of reference review	
• Conducted an annual review of the Committee's terms of reference in December 2025, considering applicable rules and best practice in the UK and Hong Kong and the ACG reforms. • Following the review, alongside the Audit Committee, the Committee recommended material changes including the transfer of the oversight of FCR and Compliance Risk from the Audit Committee to the Board Risk Committee. A new material controls responsibility was added in light of the ACG reforms to complement the oversight of the Audit Committee.	• The Board approved the proposed amendments to the Committee's terms of reference in February 2026. • Ensured the role and responsibilities of the Committee remain appropriate and align with best practice.

Source: 2025 Standard Chartered ARA

Example 19

Airtel Africa FY26 ARA, p. 116-117

Risk management and internal systems and controls

We advised the Board that our risk management and internal control systems were effective. Following its own review of the reports submitted to it, the Board agreed that our system of internal control continues to be effective in identifying, assessing and ranking the various risks we face as a business, as well as in monitoring and reporting progress in mitigating potential impact.

Our priorities	Actions taken during the year	Cross-reference
Risk management		
Looking closely at the robustness of our systems for risk reporting, assessment and control and ensuring that we focus on the areas of greatest risk	• **Reviewed and recommended the Group risk and compliance strategy** to the Board and provided oversight throughout the year, ensuring alignment with the Group's risk appetite and focus on the most significant principal and emerging risks • **Received and challenged quarterly risk management reports**, including KRI monitoring and exception reporting, to ensure early warning indicators directing management and Board attention to areas of increasing risk • **Reviewed the robustness of the risk management framework**, and confirmed that all risks on the risk register are supported by defined mitigation plans and mapped consistently to the framework • **Undertook thematic risk reviews** (including financing and foreign currency risk, IT strategy review and operational resilience, health and safety, data privacy, cybersecurity, and HR) to test the effectiveness of risk identification, controls and mitigation in areas of greatest risk exposure • **Received descriptions and updates on key controls** as part of quarterly key control status updates, enabling oversight of both ICOFR and non-ICOFR controls across the Group • **Reviewed progress on risk-related remediation programmes**, ensuring that control weaknesses identified through assurance activities are addressed and lessons applied consistently across the business	Principal risks and mitigation (p55)
Reviewing our risk management framework and conducting thematic risk reviews to ensure risk remains within our agreed appetite and is monitored and reviewed as needed to reflect external and internal changes	Conducted thematic reviews on: • **Financing and foreign currency risks** – provided enhanced oversight of liquidity, refinancing and treasury governance to inform our committee's assessment of foreign exchange, macroeconomic and capital structure risks • **IT strategy and operational resilience – risk governance and resilience** – strengthened our oversight of the implementation of the IT strategic road map, operational resilience, business continuity and disaster recovery and risk mitigation actions to support the Group's business objectives • **Health & safety** – reviewed health and safety risks related to the Group's go-to-market (GTM) mobility strategy and the embedding of appropriate risk governance controls in operational GTM processes • **Data privacy** – reviewed the Group's data privacy governance controls for legacy and new products to make sure privacy-by-design is embedded in the Group's product governance processes and the ongoing identification and mitigation of privacy risks across the organisation • **Cybersecurity** – reviewed and assessed the Group's cybersecurity posture through a quarterly update paper on the status of various cybersecurity programmes across the Group. This review also included analysing key global cybersecurity incidents reported in the public domain and assessing our own cyber practices and insights that could be used to further strengthen our internal cybersecurity controls • **Human resources** – reviewed and assessed risks with respect to the governance control framework for managing the Group's non-FTE employees. Our objective was to make sure governance controls and systems were scaling in line with the growth in the Group's business • **OpCo risk governance:** received and reviewed a report on risk perception from a survey with Group executive heads and OpCo executive committee members. This gave us insight on the strengthening of our risk management framework and risk identification process at Group functional and OpCo levels In addition to formal thematic reviews, our committee received targeted deep dives on fraud risk to support our oversight of financial crime risks and associated mitigation actions. We also commissioned focused education sessions on financial services risks to enhance our oversight of regulatory and conduct risks associated with mobile money operations.	Managing our risk (p50) Principal risks and mitigation (p55)

Our priorities	Actions taken during the year	Cross-reference
Risk management		
Clarifying processes and controls to help people identify, monitor and mitigate risk earlier and more effectively	• **Revisited and strengthened the business unit self-certification process**, reinforcing accountability for risk and control ownership at an operational level and supporting more timely identification of control weaknesses • **Clarified and standardised the use of key risk indicators (KRIs) and tolerance limits**, embedding an exception-based reporting approach so that emerging issues are escalated early to management and the Board • **Received clearer descriptions of key controls** through quarterly key control status updates, improving understanding of how controls operate in practice across both ICOFR and non-ICOFR processes • **Reviewed and challenged the quality of risk registers**, ensuring that all identified risks are supported by defined mitigation plans and consistently mapped to the Group's risk management framework • **Conducted design and compliance reviews as part of key issues reporting**, with learnings applied across the business to strengthen consistency and prevent repeat control failures • **Introduced continuous controls monitoring** and agreeing rollout across markets and business lines to enable earlier detection of control failures and emerging risk trends • **Reviewed overall ratings of process and control effectiveness across OpCos**, including end-to-end process assessments, to highlight areas needing management attention and remediation • **Policy review and approval:** reviewed and approved several governance policies setting the governance processes and standards and ensuring consistent application across the Group	
Ethics and culture		
Promoting, assessing and embedding risk and ethical culture across the organisation	• **Insights from employee focus groups on culture** – reviewed and assessed feedback from employee focus group sessions aimed at eliciting feedback on various aspects of the Group's risk, ethical and compliance culture to ensure alignment with the Group's purpose, values, strategy and business model • **Groupwide culture campaign** — reviewed the design, key principles and implementation of the Group-wide culture campaign which was rolled out across the Group and its subsidiary during the financial year. The aim of the campaign was to reinforce the organisation's business and ethical values and to highlight employee responsibilities and role in ensuring the right behaviours in day-to-day business activities and decision-making. The committee received regular updates on the progress and implementation of the culture campaign • **Whistleblowing reports** – reviewed whistleblowing reports on a quarterly basis including assessing key themes to identify any key patterns that needed to be addressed at an organisational level	
Statutory audit and audit engagement		
Reviewing the services, fees and policy for non-audit services provided by the auditor for the year	• Approved the permitted non-audit services fees provided by Deloitte for 2025/26, in accordance with the Group's non-audit services policy	Part 5 (p123)
Approving the statutory audit fee for the year	• Approved the fees for the 2025/26 statutory audit and noted that the 2024/25 statutory audit fee had been paid	Note 8.1
Internal audit and chief internal auditor review		
	• **Reviewed and approved the annual combined assurance plan**, covering second- and third-line assurance activities, to ensure assurance effort was aligned to the Group's principal and emerging risks and areas of greatest risk exposure • **Received and considered regular progress reports on assurance delivery**, including the outcomes of internal audit and other assurance reviews, and monitored management's response to findings and agreed remediation actions • **Maintained regular engagement with the chief internal auditor** to oversee the effectiveness, independence and resourcing of the internal audit function and ensure appropriate escalation of significant issues to our committee and the Board	

Source: 2026 Airtel Africa ARA

Example 20

Rolls-Royce 2025 ARA, p. 80

Effectiveness of risk management and internal control systems

The Committee has conducted a review of the effectiveness of the Group's risk management and internal control systems, including those relating to the financial reporting process. We consider that our review of the risk management and internal control systems, in place throughout 2025 and up to the date of this report, satisfies the requirements of the Code, the DTR and the FRC's guidance on risk management. To support this:

- we monitor changes to regulatory requirements with respect to risk management on an ongoing basis;
- we review relevant policies and procedures and update where necessary, in line with regulatory changes and our perspective on effective approaches to risk management;
- our risk management team and relevant assurance functions, such as internal audit, review key business processes, including long-term contract pack reviews and the budgeting process with periodic reforecasting, identifying key risks and opportunities;
- we assess and monitor management responses to key audit findings, including the design of mitigations and developments to existing controls;
- a defined anti-bribery and corruption policy has been implemented; and
- where necessary, we report to the Board and its Committees on key risk and regulatory matters.

During the course of the financial year, any control weaknesses identified through the operation of our risk management and internal control processes were subject to monitoring and resolution in line with our normal business operations. In 2025, no significant weaknesses were identified. To further support the enhancement of the existing internal control environment:

- risk management specialists have been assigned to review and monitor the implementation of actions, to ensure these remain appropriate and aligned to the risks to which they relate;
- policies and procedures are subject to review and are updated to align with changes in the underlying control environment; and
- risk owners are accountable for managing these risks.

In addition, and on an ongoing basis, the Board reviews the effectiveness of the Group's risk management and internal control system and continues to:

- monitor reports from the Executive Team, relating to their assessment of risks and internal control systems;
- monitor assurance received from the Executive Team regarding compliance with relevant policies;
- monitor assurance received on the effectiveness of the Group's internal control environment;
- review reports from this Committee, the internal audit function and the external auditor;
- review the Group's response to incidents and threats, including those related to cyber-security and safety; and
- review information gathered from the Group's formal whistleblowing process where issues relate to financial misconduct.

Where opportunities for improvement were identified, action plans have been put in place and progress is monitored by the Committee.

Source: 2025 Rolls-Royce ARA

Example 21

Bunzl 2025 ARA, p. 90

RISK MANAGEMENT AND INTERNAL CONTROLS OVERVIE

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
- consideration of 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 operating company and business area management to discuss strategic, operational and financial matters;
- the Executive Committee reviews the principal risks affecting each business area and the policies and procedures in place to manage them;
- the Board in turn reviews the outcome of the Executive Committee's discussions on principal risks, which ensures a documented and auditable trail of accountability;
- these processes culminated in the Board's approval in 2025 of a new principal risk relating to major change programme execution, reflecting the issues associated with the change programme undertaken in the Group's largest business in North America;
- 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. In addition, the second line internal controls team have an annual risk-based programme of activity involving various reviews of control compliance within the businesses;
- 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 the Group;
- the Internal Audit function annually 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 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 97 to 106;
- 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: 2025 Bunzl ARA

Example 22

Next January 2026 ARA, p. 72-73

Evaluation of the effectiveness of risk management and internal control systems

Evaluation of the effectiveness of the Group's risk management and internal control systems for all parts of the business has been carried out twice during the year. This covered all material financial, operational and compliance controls. The evaluation process involved the following:

- **Executive director review** – the most significant corporate level risks of the Group, as identified by the risk management process, and their associated controls were assessed in detail by the executive directors. The objective of this top down review was to ensure that the appropriate risks had been accurately captured within the risk management processes described above, that adequate controls were in place to mitigate these risks and that their potential impact had been robustly assessed. The executives also considered the appropriateness of the principal risks identified.
- **Audit Committee review** – at the January 2026 meeting, management presented the Committee with details of the ERMF, the risk scoring matrix methodology and the ownership and oversight of risks. The Committee also considered the nature and circumstances around significant risk events that had occurred during the year to assess whether they suggested significant failure or weakness in internal controls. An internal financial controls matrix summarising the key processes and oversight of the Group's financial controls was reviewed, with input from senior finance management. The Committee also satisfied itself that management's response to any financial reporting or internal financial control issues identified by the external auditor was appropriate. The Audit Committee also reviewed progress on the Group's preparedness for Provision 29 of the Code at its meetings during the year.
- **Board review** – at their January 2026 meeting, the Board undertook its formal review of the effectiveness of the risk management systems of the Group. Management supported this review by presenting information about the Group's risk management systems and processes, the output of the reviews undertaken by the Audit Committee and the executive directors, information about the most significant business risks and a summary of the type and regularity of key executive director-led risk governance meetings, mapped to the principal risks.

To support the Audit Committee and Board in discharging their responsibilities, they were provided with the following information:

- Relevant extracts regarding their responsibilities in relation to risk management and oversight from the Code and FRC Guidance.
- A review of the Principal Risks identified by other comparable listed companies. This helps to ensure that there are no material gaps in our risk identification or impact assessment.
- Details of the identified material controls and whether the number and types in place are comparable with other FTSE 100 companies as part of planning and considerations for Provision 29 of the Code.

Following the evaluation process described above, the Board is satisfied that, under Provision 29 of the 2018 Code (applicable for the financial year under review) the material controls have been operating effectively for the financial year ended January 2026 and up to and including the date of this Annual Report (see page 120 for further details). No significant failings of material internal control were identified during these reviews.

The business will continue to review opportunities to develop, strengthen and improve the effectiveness of our risk management and internal control systems.

Source: 2026 Next ARA

Example 23

Severn Trent 2026 ARA, p. 67

Business continuity

Security and resilience remain a Principal Risk (page 71), reflecting our responsibility to deliver essential services and protect critical national infrastructure from malicious activity. We also recognise how they are intrinsically linked to all our Principal Risks. Heightened geo-political tensions and recent high-impact cyber incidents are reflected in our Emerging Risks and PESTLE analysis. We adopt a 'when, not if' mindset, with a strong focus on preparedness and proactive risk management. Our business continuity arrangements are designed to safeguard operational resilience and customer service, while prioritising the safety and well-being of our colleagues during significant disruption.

Our Approach
Our 'Being Prepared' framework integrates incident management, business continuity and emergency planning to ensure we have the capabilities, resources and plans required to remain resilient. Sustained investment in resilience, rigorous scenario testing and strong governance oversight ensure we continue to strengthen our ability to withstand, respond to and recover from the most significant threats to our operations. The level of cyber risk exposure remains unchanged as our control environment continues to evolve in line with external threats. We have also established a Cyber Defense Committee to provide strategic leadership and decision making in the event of an incident.

Our Board
The Board has demonstrated strong leadership and a commitment to maintaining a robust security culture, supported by regular discussions on the evolving security landscape and the recognition of the continued need for investment, vigilance and responsiveness. This included a dedicated cyber readiness deep-dive, covering threat detection, incident response capabilities, supply chain dependencies and data governance arrangements. During the year the Board also participated in a cyber incident simulation, with further details set out on page 93. The exercise was designed to replicate the pressure, pace and uncertainty of a real cyber attack, strengthening Board-level preparedness and decision making.

Examples of business continuity activities

Before

- Our security and resilience framework provides an integrated approach to identifying threats and strengthening resilience, supported by a dedicated cyber security function.
- Business impact analysis informs the identification of critical services, with robust continuity plans and defined service-level agreements for business-critical IT.
- Long-term strategic investment in people, processes and technology ensures our security capabilities continue to evolve in line with the changing risk landscape, with a strong focus on proactive cyber controls to reduce exposure.
- Clear accountabilities, including a Chief Information Security Officer, which are supported by regular awareness and training. Company-wide exercises ensure colleagues can identify threats and respond effectively.
- Our arrangements are regularly tested, including Board-level involvement and support from external partners, providing an opportunity to test key areas including decision-making, escalations and crisis communications.
- The Board and management also engage with external networks to share intelligence and best practice, strengthening collective preparedness.

During

- In the event of an incident, the appropriate operational, tactical or strategic teams are activated immediately. Clearly defined roles and responsibilities enable a coordinated and efficient response, supported by processes that have been consistently proven to be effective.
- Robust communication protocols ensure timely engagement with operational teams, the Board, regulators and key third parties. This enables clear oversight and support throughout the incident lifecycle.
- Established decision-making pathways focus on rapid containment and prioritisation, safeguarding the continuity of essential services.
- Rotas are in place to protect colleagues' well-being and ensure sufficient resources are maintained across critical activities.

After

- Post-incident reviews are undertaken following all exercises and any activation of the incident management process.
- Relevant security breaches across all sectors are reviewed to understand the root cause and emerging themes. The effectiveness of responses are evaluated to identify areas for improvement and further strengthen organisational resilience.
- Reporting is provided to stakeholders, setting out the incident timeline and ensuring that lessons learned are captured, shared and addressed on a timely basis.

Source: 2026 Severn Trent ARA

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.

EYSCORE 112780-26-UK
ED None

UKC-044138.indd (UK) 06/26.
Artwork by Creative UK.

ey.com