The Goldilocks phase and beyond

Provision 29 of the UK Corporate Governance Code

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

EY
Shape the future with confidence

Provision 29 – the Goldilocks phase and beyond

In brief:

Revised Provision 29 introduces a requirement for boards to monitor and review the risk management and internal control framework and declare the effectiveness of material controls. However, this is not a regime; there is no prescribed methodology, and companies must design proportionate responses suited to their risk profile and control maturity.

Companies are now in the 'Goldilocks phase', calibrating their approach – refining material control populations, enhancing information flows, validating project design through internal and external input and benchmarking against peers to confirm they are doing not too much, not too little, but just enough for their circumstances.

Material controls tend to fall into four categories – entity-level controls, elevated key controls, single-risk frameworks and cluster controls (the latter two underpinned by key control activities). Organisations 'pick and mix' from these categories based on control maturity and risk significance.

Effectiveness assessments require tailored criteria by category, supported by confidence strategies that consider outcome-indicators, attestations or testing. Dry runs help companies surface gaps and refine judgments before the first declaration.

Boards will need to exercise judgement when making the declaration: an effectiveness criterion not being met does not automatically render a material control ineffective. Directors will need to consider key risk indicators, risk appetite and scenario analysis before deciding whether disclosure of ineffectiveness is needed.

Next steps focus on readiness for 2026/27, including securing agenda time, running post-dry-run debriefs, finalising board reporting format, drafting disclosures, pre-agreeing declaration wording and validating whether material control populations, criteria and confidence strategies identified in the preparatory phase remain appropriate for the year ahead.

Authors

Mala Shah-Coulon
Partner
Audit Regulatory and Public Policy
Ernst & Young LLP
mshahcoulon@uk.ey.com

Maria Kępa
Director
Audit Regulatory and Public Policy
Ernst & Young LLP
mkepa@uk.ey.com

On 19 January 2026, the government announced that it will not progress the Audit Reform and Corporate Governance Bill. This decision does not impact the requirement in the 2024 Corporate Governance Code for commercially listed companies to apply revised Provision 29 on risk management and internal control.

Contents

1. Introduction

Provision 29 of the UK Corporate Governance Code requires boards to monitor and review the effectiveness of their risk management and internal control framework throughout the year, set out how they have done this and make an annual declaration on the effectiveness of material controls. In December 2018, Recommendation 51 from the **Independent Review of the Financial Reporting Council** ('the Kingman Review') noted that 'serious consideration to the case for a strengthened framework around internal controls in the UK, learning any relevant lessons from operation of the Sarbanes-Oxley (SOX) regime in the US' should be given.

Seven years later, requirements that began as a conversation about introducing a UK SOX-lite for all public interest entities are finally in effect. The outcome, however, is very different from the starting point.

The changes were introduced through updates to the UK Corporate Governance Code (the Code), not through legislation. As such, the requirements operate on a comply or explain basis and are limited in scope to those companies applying the Code. This means that far from being a regime, like US SOX, there is no prescribed methodology for dealing with the new Provision 29, no enforcement mechanism and no associated auditor's opinion. Companies and their boards are expected to figure out for themselves the approach that is best suited to their circumstances. For organisations with mature control environments, this can mean very limited enhancements to existing internal practices. Often, these enhancements centre on improved information flows to directors to enable more robust board-level discussions.

The final changes to the Code differ significantly from both the initial 2018 conversation and the draft version consulted on. As a result, some confusion remains about what directors must actually do. In our view, directors:

Should	Are required to	Are not required to
Define what is meant by 'material control' for the company and the board	Agree on the material controls for the company[1]	Disclose the definition of material controls Disclose the material controls of the company, other than if a material control is ineffective as at the year-end (Provision 29c)
Agree what 'effectiveness' means for each material control and what the board needs to confidently reach a conclusion on effectiveness	Provide an outcomes-focused disclosure (Principle C) to help the reader understand how the board monitors and reviews the entire risk and internal control framework (Provision 29a)	Obtain assurance over all or any of the material controls Disclose what assurance has been obtained over the material controls Disclose why a material control was deemed not to be operating effectively
Agree how outcomes of management's monitoring and review of material controls will be provided to the board	Provide a declaration of material control effectiveness as at the year-end (Provision 29b)	Provide a declaration of the effectiveness of the entire framework

1 This is an inferred, not an explicit requirement.

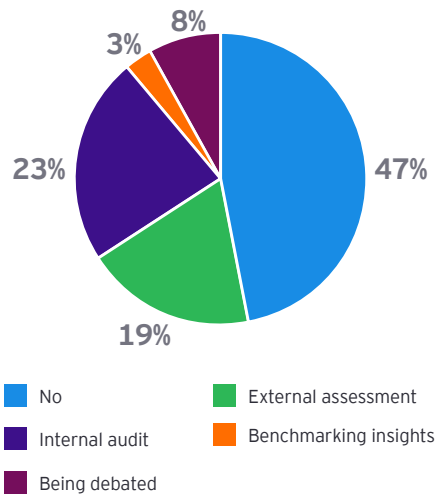
89%

of boards expect to approve the list of material controls

15%

also request insight into underlying key controls

Boards asking for validation of the project design, programme and governance



For companies with a 31 December year-end, preparations are now in full swing. Most boards have received multiple briefings. In some cases, these included walking through several material controls as a proof of concept and agreeing the format in which information will be presented to directors. Many boards have now reviewed initial lists of material controls and shared their views and challenges back with the teams.

The roundtables and individual meetings we held in winter 2025 indicate that many of the well-advanced companies are now entering the '**Goldilocks phase**' of their projects. They are finetuning the approach to confirm they are not doing too much or too little but getting it just right for them. Throughout this publication, we have highlighted **using bold text** the deliberations and challenges and the resulting refinements and calibrations companies have been making in the Goldilocks phase.

Companies focus on sufficiency and proportionality, while applying learning on how to enhance less mature controls. Companies are engaging with control operators and increasing education to confirm that any enhancements remain useful for business-as-usual operations.

Some boards are asking for validation, either from internal audit or from an external provider, of the project design, programme and governance. Directors are also keen to understand the approach taken by peers, with some seeking market insights and benchmarking from their external auditor including a high-level sense check on the material controls identified and whether any obvious risk areas that warrant a material control have been inadvertently omitted.

Furthermore, many companies are conducting a 'reporting dry run' as part of the 2025 year-end audit committees, moving theoretical considerations into practice. As companies assess the effectiveness of material controls and apprise non-executives about the approach, they grapple with granular questions and challenges of operationalisation.

With less than a year before the first declarations are going to be made public, we decided it would be most helpful to share insights promptly, without waiting to supplement these with an analysis of disclosures in the latest annual reports. This update to our ***On track for Provision 29 compliance*** publication is therefore based on interactions we and other EY colleagues have had with FTSE100 and FTSE250 companies in the second half of 2025. It builds on and succinctly reiterates the core observations from our earlier work and supplements them with the most recent developments, which we have clearly highlighted.

Our insights draw on direct interactions with more than 100 commercial listed companies across various industries. In addition, in January 2026 we surveyed a similar number of companies preparing to comply with the revised Provision 29.

Goldilocks and the Three Bears

This is a classic fairy tale in which a curious girl enters the home of three bears and tests their belongings – porridge, chairs and beds – rejecting extremes ('too hot', 'too cold', 'too hard', 'too soft') until she finds the option that is 'just right'.

Traditionally a cautionary story about respect, boundaries and venturing into the unknown, it has evolved into a powerful metaphor for the search for an optimal middle ground – a state of balance between two extremes.

This 'just right' principle now underpins thinking in fields such as psychology (moderation), economics (steady, sustainable growth), and science (the 'Goldilocks Zone' where life can exist).

2. Material controls identification

From quite early on, companies identified material controls by reference to enterprise risks and disclosure risks, and this approach continues to dominate.

Material controls are not simply a subset of what would be classified as 'control activities' under the COSO framework.[2] Many of them span multiple components of an organisation's risk management and internal control systems. They aggregate a variety of activities to create overarching mechanisms able to address a particular risk across the business. Control activities executed by the first line often underpin material controls. These activities respond to risk at the level of individual transactions, actions or processes and are commonly referred to as underlying key (or critical) controls.

86%

have identified material controls against each principal risk

48%

map some material controls to risks a tier below principal risks for more meaningful oversight

2.1 Enterprise risks

Principal risks confirmed by the board under Provision 28 are the most common starting point to identify material controls over enterprise risks. Over time and in response to challenges from boards, companies became more confident that not all principal risks require material controls. Instead, they began focusing more on risks to the viability of the business. A few undertook a reverse stress test exercise to home in on principal risks requiring most attention. They also sought to identify any black swan events where the probability of occurrence is sufficiently low as not to qualify as principal risks, but the impact is so high that viability could be threatened should they occur.[3]

Risk articulation has also improved to become more company-specific. This was especially the case for risks outside of a company's control, with the emphasis now on preparing to respond to events in a timely manner. This led some companies to identify material controls related to the development of resilience and business continuity plans and putting the right mitigants in place. To increase precision, companies also more commonly identified material controls against risks a tier below principal risks, as illustrated in the cyber risk example in Section 5.

Although most companies used their principal risks population as a starting point to identify material controls, some took a different approach as illustrated by the quote below.

2 Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control – Integrated Framework

3 A reverse stress test:
a. Starts from the assumption that the company has become unviable

b. Identifies the qualitative circumstances that could have led to that outcome

c. Constructs a scenario of events that could lead to those circumstances

d. Works back to determine the probability of that scenario occurring, despite the mitigating actions at the company's disposal

“

I have always considered risk to be the effect of uncertainty on objectives. Provision 29 provided us with the trigger to shift our consideration of controls from a traditional risk-centric approach to an objective-centric framework. The framework we now use is centred on the following five elements: objectives, risk, controls, assurance and actions.

The traditional view is that all risk is negative and must be managed to protect the business. This objective-centric approach has helped us consider controls both to protect the business and help it grow. This shift has enabled the risk and control functions to have more meaningful engagement with stakeholders in our business and even helped with our business case to make specific investments, for example, in control systems.

From a practical perspective, this has also led us to expand the traditional controls we examine within processes. We now also consider controls at a policy and project level. These often address different time horizons and risk profiles and generate both immediate and systemic benefits. For example, our staff may be able to do something value-accretive immediately. Over time, we may be able to streamline or even rationalise controls across several processes because a project control deals with the risk more efficiently.

– Head of Risk and Governance, major UK retailer and consumer services provider that voluntarily applies the UK Corporate Governance Code

2.2 Disclosure risks

Disclosure risks cover both financial and non-financial reporting included in annual reports, sustainability reports and similar publications. They also cover price-sensitive information disseminated through the Regulatory News Services (RNS), investor, analyst and capital market presentations. In response to Provision 29, companies have been expanding the remits of their disclosure committees to include oversight of all these aspects of corporate reporting. Alternatively, they are setting such committees up and formalising the underlying information flows and processes for the management of inside information where these were not already in place.

2.2.1 Financial reporting

As illustrated **by Companies A and B below**, the approach to material controls over financial reporting varies significantly between companies depending on the maturity of their internal controls over financial reporting (ICFR) framework. Many companies decided how to address financial reporting in the earlier stages of the Provision 29 compliance project and made few substantial changes, if any, as preparations progressed. In some cases, this has meant continuing to develop the control environment to meet the predetermined target model in time for the first declaration.

2.2.2 Non-financial reporting

The thinking regarding non-financial reporting, on the other hand, has been evolving significantly. Initially, many companies were concerned about the immaturity of the processes supporting sustainability reporting, the breadth of related disclosures and what this might mean for making the declaration.

Over the last months, however, many companies have pivoted towards concluding that only a few sustainability disclosures are in fact price-sensitive or influence investment decisions. This can involve engaging with investors to understand what information actually impacts their decisions, and monitoring what disclosures by them or their peers influence share price. For those one or two topics that truly matter, the combination of underlying operational-related controls, for example, in respect of health and safety or modern slavery prevention, with disclosure committee oversight is seen as sufficient. This reflects a proportionate, risk-based approach that focuses material controls where disclosure risks are genuinely material to the entity.

Sometimes companies bolster this by obtaining external assurance, especially when wanting to safeguard against the risk of greenwashing. The right external assurance provider will scrutinise selected disclosures and confirm they are not obviously wrong. With current levels of immaturity, many companies see the process of obtaining voluntary assurance not only as a source of confidence over the accuracy of their own disclosures but also as a means of correcting mistakes before information is made public. In this context, selecting the right assurance provider and the scope of assurance could be a material control, rather than the fact of obtaining assurance.

Delayed disclosure of inside information

In its October 2025 newsletter for primary market participants (No. 59), the Financial Conduct Authority (FCA) reported the outcomes of its review of issuers' compliance with Article 17.4 of the UK Market Abuse Regulation (UK MAR), which permits issuers to delay the public disclosure of inside information under certain conditions. The FCA noted a 39% decrease in delayed disclosure of inside information (DDII) notifications submitted per day compared with its previous review. It acknowledged that factors such as market conditions may affect the volume of notifications, but stated that such a significant drop was unexpected. While recognising that the decrease may not indicate a fall in compliance levels, the FCA reminded issuers to ensure they have appropriate arrangements in place to meet the requirements of Article 17.4 of UK MAR.

“

Why does finance need to be involved in sustainability reporting?

Sustainability is evolving from being an undefined corporate bolt-on to being an organisation-specific, integrated element of core business and functional operations. Gone are the days of corporate social responsibility; the focus is now on policies that lead to operational and strategic resilience, driving and underpinning economic value as part of business as usual.

The same is now true when it comes to sustainability reporting. As a company's storytelling expands from financial performance to other areas, business is investing in cost-effective reporting capabilities that need to be compliant and withstand investor, regulatory and assurance requirements. Finance teams are well placed to support this shift.

Any material controls related to sustainability reporting should draw directly on the underlying key controls within the related operational processes. If you take modern slavery considerations in the retail industry as an example, businesses should already have policies and processes in place to prevent and detect modern slavery. Provision 29 is an opportunity to strengthen these controls rather than introduce multiple underlying controls relating purely to reporting and disclosure.

If the operational controls are fit for purpose, finance teams can leverage existing capabilities to support data integrity. Their expertise in interpreting reporting frameworks and managing controlled, consistent data collection is increasingly essential across both financial and non financial domains.

As a result, controllership is becoming a discipline that spans the full spectrum of corporate reporting, both financial and non-financial.

– Joe McMullan, Director, Enhanced Corporate Reporting
jmcmullan@uk.ey.com

Regulatory compliance and legal risk

Many companies are still grappling with determining the right approach to material controls over regulatory compliance and other forms of legal risk. Although policies, delegation of authority (DoA) and standard contract clauses might be in place, confirming these are adhered to and evidencing that this is the case is proving challenging.

As part of Provision 29 projects, some companies are investing in enhancing their contract repository databases and introducing self-attestations to confirm adherence to DoA at business-unit level. They are also considering how to enhance compliance monitoring. Confirming the completeness of the population of contracts and business partners remains a concern. Companies increasingly include rates of relevant training completion in the material control effectiveness criteria. They do this to emphasise the importance of educating the workforce about the need to appropriately consult with legal teams, adhere to DoA and securely store contracts.

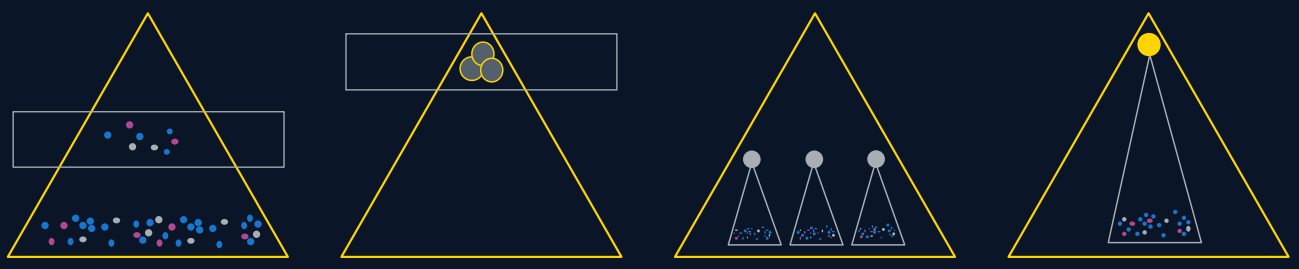
This illustrates a recurring Goldilocks challenge: calibrating the right level of response proportionate to risk and control maturity.

3. Material control categories: the ‘pick-and-mix’ model

Based on our work with FTSE 100 and FTSE 250 companies, we observe that organisations are selecting material controls from four main categories. As outlined in our *On track for Provision 29 compliance* publication, we call this the pick-and-mix model – a term we use to describe the diverse approaches we see in practice. When we stepped back and analysed what companies were identifying as material controls, we found they naturally fit into four types. By naming and defining these categories, we aim to create a common language for discussing different approaches. Companies choose the combination of control types that best fits their specific circumstances and control maturity, rather than following a single prescribed approach. Most organisations select from entity-level controls, single-risk frameworks, cluster controls and elevated key controls, using a combination across different risk areas, hence pick-and-mix, rather than applying a single category uniformly.

The four categories operate as follows:

Market practice – categories of material controls (pick-and-mix model)



Elevated key controls
‘Dip down’ into individual key process-level controls

Entity-level controls
Organisation-wide controls that establish a pervasive control environment

Cluster controls
Groupings of controls (prevent, detect, compensating) often monitored by an executive committee or risk owner

Single-risk frameworks
A specialised subset within the overall risk management framework, focused on a specific principal risk

Cluster controls and single-risk frameworks are underpinned by key controls (typically control activities within the first line). Elevated key controls are a subset of such controls, whereas entity-level controls operate top-down.

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

4 COSO definition: Entity-level controls operate at the organisation-wide level to establish the tone, culture and processes that support the internal control system, including governance, risk management and oversight activities. While other definitions exist, these are not UK-specific.

A **single-risk framework** functions as a specialised subset within the overall risk management and internal control framework, focused on a specific principal risk (or the tier below). It is the most comprehensive way to evidence that a risk is being managed. It operates under the governance structure of the overall framework, adhering to its risk appetite, Three Lines Model and reporting lines.[5] It uses the same methodologies (e.g., risk assessment scales, likelihood-impact matrices) to maintain compatibility and will often include one or more entity-level controls or their elements. A single-risk framework can be localised to the needs of a particular country or business unit.

A **cluster control** comprises prevent, detect and compensating controls related to a narrower risk area. A risk owner (such as an individual, an executive risk committee or a regional/divisional forum) monitors the combined effectiveness of these controls by overseeing key risk indicators, control assurance results and other metrics. This oversight mechanism is referred to by some organisations as a governance or oversight control and designate it as the material control. However, referring to the entire grouping as a cluster control highlights the dependence of the governance control on the underlying key controls. It emphasises that a risk can remain in check even if an individual prevent key control has not operated, provided other controls within the cluster detected the issue.

Elevated key controls are controls within individual processes that meet traditional definitions of control activities. Management uses a standard control documentation format for them. Management considers that such controls individually play a very significant role within the organisation's risk management and internal control framework. As elevated key controls are only a subset of all key controls addressing a particular risk, they may need to supplement them with an entity-level material control.

The choice of category is predicated on the maturity of the control environment in respect of a given risk area. **This is another Goldilocks consideration. Single-risk frameworks may not have been embedded in emerging control environments; elevated key controls alone may be an inefficient approach for mature organisations. The aim is to match the category to circumstances: not too much, not too little, but just right.**

Generally, single-risk frameworks address risks most comprehensively but require significant control maturity. Where maturity is lower, or where risks are changing rapidly and require closer monitoring, cluster controls offer a more flexible approach. Elevated key controls, often supplemented by entity-level controls, may be the only viable option for organisations with less developed control environments. As such, companies are likely to pick-and-mix material controls from within the categories to best reflect their circumstances.

In practice, this means that companies with mature control environments that have progressed well the journey towards Provision 29 compliance tend to identify:

- A suite of material controls related to disclosure risks, typically owned by the finance function, even when relating to non-financial disclosure, supplemented by a disclosure committee. Greenhouse gas emissions are among the most common non-financial reporting disclosure specifically under consideration.
- A few entity-level controls, mainly dealing with setting the tone at the top (linked to the code of conduct and speak-up arrangements) and overall direction of travel for the organisation (strategic business plans or resilience planning). Some organisations, especially those that are subject to US SOX, do not separate out the former into individual material controls, but consider them as part of the material control related to their ICFR framework.
- A combination of framework and cluster controls covering the majority of (but not necessarily all) principal risks, with some of the controls pinned to the risk tier below. These tend to be for the entire organisation, often with a clearly identified board sponsor, risk owner, control champion and objective owners, rather than specific to a business unit or division.

We recommend classifying material controls into categories, whether aligned with those in our pick-and-mix model or ones developed internally. This drives consistency in control documentation and in effectiveness considerations within a particular category. This in turn helps explain the logic behind management's proposals to the board and pre-empt challenges about seemingly inconsistent confidence strategies.

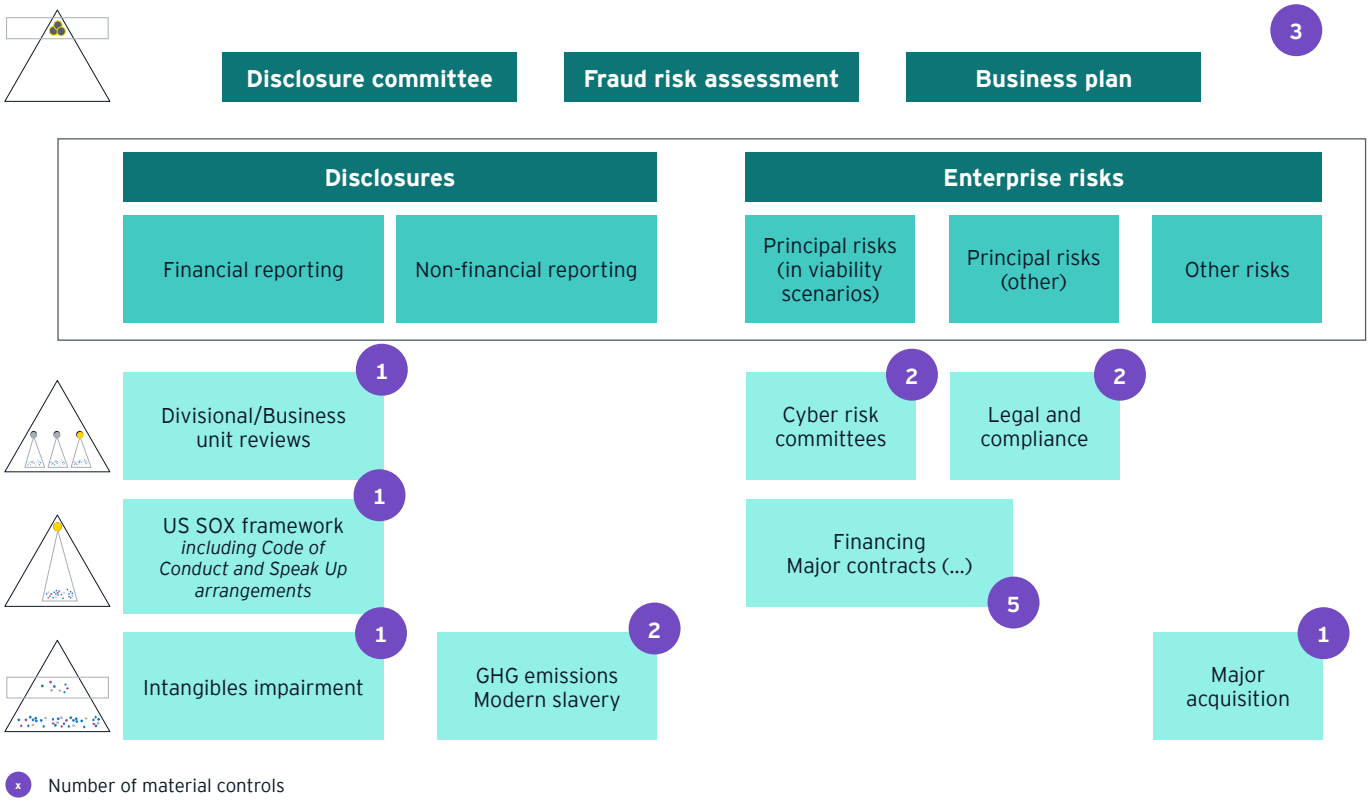
5 The IIA's Three Lines Model: An update of the Three Lines of Defence, The Institute of Internal Auditors, 2020.

3.1 Pick-and-mix model – illustrative examples

The following theoretical examples illustrate the approach by explaining the key differences between Company A that has identified 17 material controls and Company B that has identified 31 material controls:

Pick-and-mix model in practice

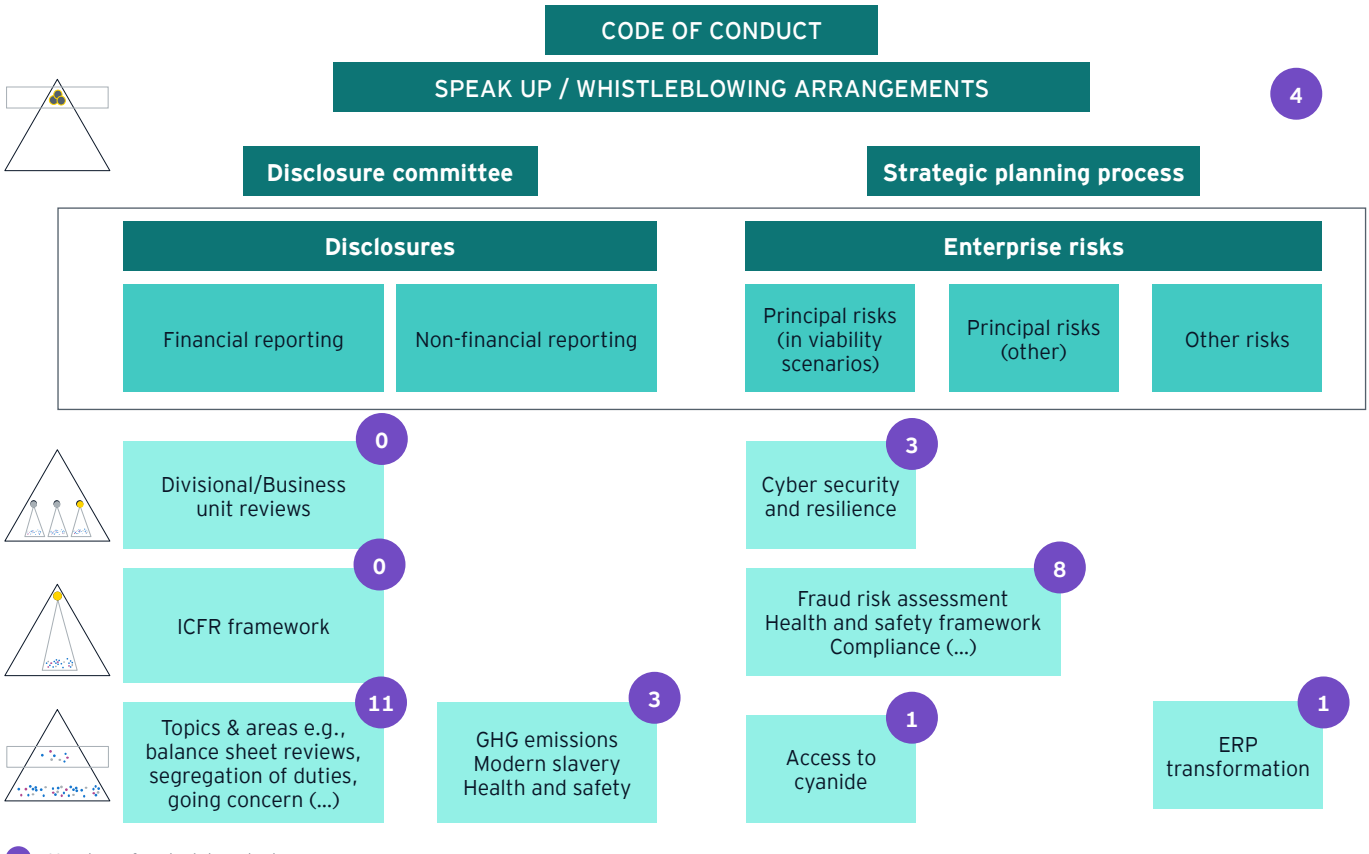
Company A



x Number of material controls

Pick-and-mix model in practice

Company B



x Number of material controls

Company A relies on its US SOX framework as the material control over ICFR, additionally pulling out an elevated key control to address its particularly market-sensitive disclosures relating to intangibles impairment. The US SOX framework incorporates several entity-level controls, for example, related to whistleblowing. Furthermore, the ICFR of a newly acquired business is controlled at the level of the related business unit, as it has not yet been fully integrated into the existing ICFR framework. Company B's financial reporting environment is not as mature, so it has identified several elevated key controls across its operations.

Company A considers its fraud risk assessment to be an entity-level control, with fraud considerations embedded across its various activities, whereas Company B identifies fraud as a principal risk, given specific legislation relevant to its business and country of operation, and has a single-risk framework in place to address it.

Both companies identify cyber as a principal risk and put in place an approach based on the National Institute of Standards and Technology Cybersecurity framework (**NIST CSF**). However, Company A has a cyber risk committee operating at each of its two business units and overseeing related control clusters, whereas Company B has established cluster controls for each of its three sub-risks – regulatory compliance, IT network penetration and third-party management.

Company B has a single risk-framework dealing with compliance risk overall, unlike Company A, which deals with compliance related to sanctions and anti-bribery matters separately from GDPR and other aspects.

36

The average number of material controls outside financial services, with an increasing number of organisations in the 20–30 range

3.2 Declining number of material controls

As the examples above illustrate, there is no right or wrong number of material controls, and this will always be company-specific. Nonetheless, the number of material controls has been reducing over time, reflecting a higher degree of aggregation in the way that material controls are articulated. Even in banking, where a year ago numbers often exceeded 100, the new range is now between 30 and 40.

Banks were previously designating more key controls as material, reflecting board obligations stemming from other regulatory requirements. Now they are choosing to focus on risk management frameworks and entity-level controls, with only a few elevated key controls, often related to trading activities, remaining. This does not necessarily mean a reduction in the number of underlying key controls; in fact, for some banks, this number has been going up.

This evolution reflects companies finding their Goldilocks balance: not too many controls, not too few, but just enough for their circumstances.

Furthermore, the number of material controls will continue to fluctuate as businesses change and evolve. For example, a company may introduce a business unit cluster control in the lead-up to the full integration of a material acquisition into its ICFR framework, as illustrated in the Company B example above. Material controls may also be identified in respect of significant projects or transactions.

"

Over time, I've seen that the effectiveness of material controls depends less on volume and more on fit. The discipline is in tailoring controls to the organisation's maturity and risk profile, so oversight remains robust without becoming burdensome.

– Neil Mathur, Partner, Risk Consulting
nmathur@uk.ey.com

4. Material control effectiveness

49%

of companies are still finalising their approach to effectiveness assessment

Originally, the Code consultation proposed that the annual report should include a description of any material weaknesses or failures identified. However, these suggestions were subsequently removed and replaced with a description of material controls that have not operated effectively. As such, instead of introducing definitions and thresholds for material weaknesses or failures, companies can focus on determining what it means that a material control is operating effectively.

Effectiveness criteria have sometimes ended up being the acid test for whether initially identified material controls were indeed so. Teams realised that they were in fact processes or 'tools' (e.g., employee assistance programmes or employee surveys) that could not be meaningfully assessed for effectiveness. Another common example is insurance policies, a very important mitigant rather than a control and one whose effectiveness can only be determined post event. Companies have therefore had to refine the articulation of designated material controls, focusing instead on the activities in place to confirm that, for example: the insurance cover is current; it is being updated for changing circumstances; that all pre-conditions are being met; and the policy has not been invalidated. Furthermore, when presenting the proposed effectiveness approach to the board, project teams often found themselves being challenged by directors as to why this varied between different categories of material controls.

Material control effectiveness criteria are best determined in parallel with the identification of material controls and with input from control owners and operators. They are not in any way prescribed and they will vary between material controls and companies. However, explicitly allocating material controls to categories, for example, those defined in our pick-and-mix model, and streamlining the approach to effectiveness within each category, can make the justification for the overall approach logical and therefore easier to understand.

Below we set out suggestions on how companies could seek to make effectiveness considerations uniform by control category. **Getting effectiveness criteria right is another Goldilocks test: not too stringent, not too loose, but calibrated to give boards genuine confidence.**

For avoidance of doubt, there is no explicit requirement for companies to conduct testing activities as part of their effectiveness assessment.

4.1 Effectiveness criteria for entity-level controls

As illustrated by a code of conduct-related example in our **On track for Provision 29 compliance** publication, a policy or standard in of itself cannot be a material control; it requires other elements, such as communication, awareness training and monitoring of adherence. Effectiveness considerations should be determined for each element and could include:

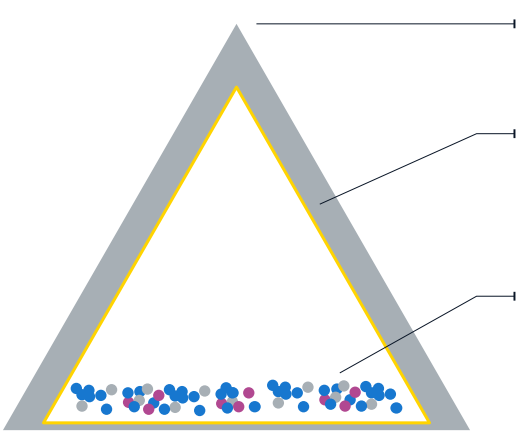
Element	Effectiveness considerations
Documented policy or standard	▪ Approved by those with appropriate level of seniority ▪ Up to date (addressing changes in the business and external changes) ▪ Includes considerations related to the relevant risk ▪ Endorsed by those with appropriate level of seniority
Communication and training	▪ Disseminated actively to all relevant members of the workforce, including new joiners ▪ Regularly reinforced via internal communications and easily accessible
Monitoring of adherence	▪ Training completion is monitored and followed up on ▪ Violations of policy/standard are followed up on or investigated ▪ Enforcement mechanisms, including disciplinary actions, are in place for violations

4.2 Effectiveness criteria for cluster controls and single risk frameworks

The approach to the effectiveness of cluster controls and single-risk frameworks involves considering their two core elements:

1. An assessment of the attributes of the material control
2. A confidence strategy in respect of any underlying key controls

Components of single-risk framework and cluster controls



Board-level monitoring and review

Material control attributes

- See 4.2.1 for cluster controls
- See 4.2.2 for single risk frameworks

Underlying key controls
require the following considerations:

i. Indicators used to monitor operational outcomes (including near miss reporting where relevant)
ii. Confidence strategy (basis and frequency)
iii. Remediation activities

4.2.1 Cluster controls

Cluster controls require an oversight mechanism that is formalised through terms of reference or role description setting out attributes such as:

- Clear responsibilities and accountabilities specific to controls
- Authority to effect change
- Information flows, including for escalation of issues
- Defined cadence of activities, including for periodic reporting to the principal risk owner or similar

Typical effectiveness criteria for cluster controls include:

- Comprehensive and up-to-date terms of reference/role description
- Duties discharged based on appropriate information (meeting packs, action-oriented meeting minutes or equivalent)
- Timeliness of remediation activities and their extent

In many cases, the governance mechanism over the cluster control may discharge duties broader than those relevant to the material control. These aspects of oversight do not need to be covered when assessing the effectiveness of the material control.

4.2.2 Single-risk framework controls

The attributes of a single-risk framework tend to be based on how the overall risk management and internal control framework is structured and, therefore, are likely to be consistent for each risk. Attributes of a framework control often include:

- Policy and standards
- DoA
- Defined risk appetite
- Designated risk owner or risk management committee
- Defined activities across the three lines
- Periodic reporting to those charged with governance

Typical effectiveness criteria for framework controls include:

- Attributes in place and up to date
- Self-regulation (responsiveness to operational indicators and other sources flagging actual and potential issues)
- Time to remediation

4.2.3 Confidence strategy for underlying key controls (and elevated key controls)

An effective single-risk framework needs to be self-regulating; an effective cluster control requires the governance mechanism(s) overseeing the cluster to discharge its responsibilities. In either case, this is predicated on:

- Having clarity on what the underlying key controls are
- Being able to identify issues with underlying key controls, including using indicators used to monitor operational outcomes and near miss reporting, where relevant
- Achieving their timely remediation

Developing a confidence strategy

There is no right or wrong approach to assessing the effectiveness of underlying key controls. The basis of the assessment can be:

- Assumed based on outcome-indicators
- Self-assessed and attested
  Or
- Tested

The frequency of assessments can be annual, on a rotational basis or ad hoc (following a risk-based plan or responding to outcomes of second-line monitoring).

Companies need to determine the confidence strategy that is best suited to their needs. This will likely vary both by control category and risk. For example, key controls addressing reporting, financial, technology and similar risks tend to be better defined, often documented within GRC tools and generally more mature. They are, therefore, more likely to lend themselves to testing than those addressing operational and compliance risks, for which self-attestations may be more appropriate.

The confidence strategy itself requires Goldilocks thinking: not testing everything, not relying solely on attestation, but calibrating the approach to control category and risk magnitude.

Preparation for Provision 29 is an opportunity to improve evidencing the operation of key controls and the consistency in how this is validated and documented.

	Key considerations	If testing
Single-risk framework	Assume that the activities across the three lines are already responsive to risk levels and that you will not need to adapt your confidence strategy	Explore a rotational approach and testing throughout the year to manage workload if the number of underlying key controls is going up
Cluster controls	Base confidence strategy on the nature and magnitude of the risk to achieve the most appropriate resource allocation and risk coverage	Remain flexible to respond to outcome indicators
Elevated key controls	Base confidence strategy on the level of reliance placed on the individual control For controls related to year-end disclosures, the timing of any confidence activities is likely to be less flexible	A rotational approach may be less appropriate than for other categories

“

Financial services institutions that are subject to SOX or that have mature ICFR frameworks, are choosing to or are in fact required to test a large proportion of their underlying key controls. Some banks and insurers had already been setting up dedicated independent teams within the first line to perform controls testing, with Provision 29 giving a further impetus to build them out. Where this is the case, the second line often sets testing standards and methodologies and coordinates the process, while the third line provides additional independent assurance. This centralised approach maintains consistency, reduces duplication and allows the second line to focus on residual risk. Some companies are also starting to experiment with automation and artificial intelligence (AI). This can include AI developing and enhancing testing scripts, performing data integrity checks in controls libraries and reviewing control wording.

Those further along in the process are reporting improved accountability and efficiencies as control operators identify ways to reduce the volume of evidence they must retain and share for testing.

– Cassondra Polegri, Financial Services Partner, Climate Change and Sustainability Services (CCaSS)
cpolegri@uk.ey.com

Weaknesses in underlying key controls
Teams are debating how to translate weaknesses in individual key controls into effectiveness considerations of the related material controls. We consider that looking to US SOX might be unhelpful, especially when the impacts cannot be expressed solely in monetary terms.

In our view, numerous or very serious problems in the effectiveness of multiple underlying key controls undoubtedly require consideration. However, they do not automatically equate to material control ineffectiveness. To the contrary, the fact that issues are being picked up and promptly remediated indicates that framework and cluster mechanisms are working as intended.

Nonetheless, where companies take a different approach to such weaknesses, we advise against bright-line breach thresholds that lead automatically to an ineffectiveness conclusion. Increasingly, companies are seeing Provision 29 compliance less as an exercise to determine control effectiveness in the traditional sense and more as a means of establishing that there is a solid basis for board-level discussion and being able to conclude that a company is operating within its stated risk appetite.

For single-risk frameworks, the risk or control owner will need to consider various data points in the round. For cluster controls, the governing mechanism must do likewise. They should not look at key prevent and detect controls in isolation and should exercise judgement before making a recommendation to the board.

Similarly, when engaging internal audit or an external assurance provider to assess the effectiveness of material controls or key underlying controls, companies should structure the engagement carefully. In many cases, there will not be a binary 'pass or fail' outcome that directly translates into a disclosure within the declaration. The assessment should rate each of the effectiveness criteria individually, rather than providing an overall rating, as discussed further in Section 4.2.1.

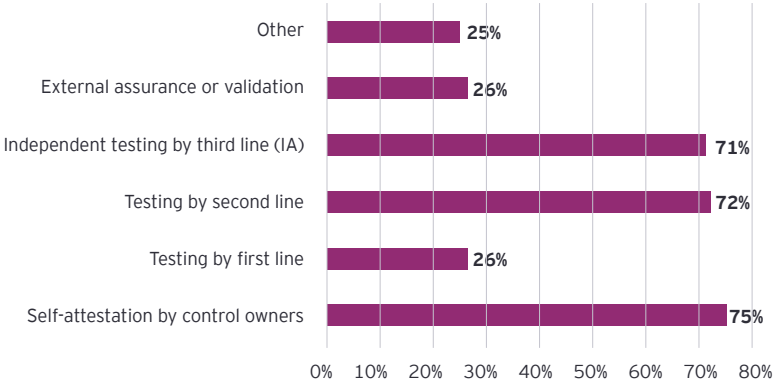
86%

of companies are conducting or planning a dry run

4.3 Dry run considerations

Companies that were planning or had already commenced dry run activities were often focusing predominantly on executing the agreed-upon confidence strategy, including testing underlying key controls. In many cases, the primary objective was to identify and subsequently remediate any effectiveness gaps.

Determining effectiveness of material controls



However, a dry run could also be an opportunity to calibrate and fine-tune effectiveness criteria. By performing a backward look and applying today's criteria to the previous year, some companies are determining whether they would need to disclose any material controls as not operating effectively. They are also considering whether, with hindsight, that would be a proportionate outcome.

5. The board declaration on material control effectiveness

To date, directors have been highly engaged in the preparatory process. They have actively challenged and refined the population of material controls to focus on risks that can bring the business down. They have emphasised the importance of leveraging control mechanisms and confidence activities that already exist. Directors have also encouraged management not to treat this as a tick-the-box exercise in compliance.

As companies move towards making their first declarations, the Goldilocks principle applies again. Disclosure must be neither too detailed nor too generic, but appropriately informative and proportionate.

5.1 Monitoring and review by directors

In most cases, management intends to report to the board on Provision 29 via the audit committee. This is the case even when other board committees have specific responsibilities over particular risk areas, such as health and safety, climate change or technology. It is possible that this approach may change in future years, once the audit committee is satisfied that the overall approach is cohesive, coherent and being executed appropriately.

5.1.1 Supporting information

Determining the timing and format of supporting information needed by directors to monitor, review and conclude on the effectiveness of material controls is still in its early days. The ongoing dry runs should include management presenting sources of confidence to the board in the intended manner. This will allow directors to ascertain whether the information is appropriate and the proposed format is adequate to support them reaching a conclusion on effectiveness. It will be of paramount importance to strike the right balance between providing sufficient information and not treating directors like executive management.

Sharing confidence maps with directors has so far been a useful part of developing the proposed approach to effectiveness. It helps visualise existing coverage and enables directors to ask more targeted questions about the confidence strategy and how it improves resource allocation. Some directors even expect management to take them through plans for the testing of underlying key controls in detail.

Many companies intend to provide confidence maps to the board regularly. This will have two main objectives: to summarise what happened during the year as part of the review and to set out the plan for the year ahead to agree the forward look for scheduled monitoring activities.

In addition, especially in financial services, management intends to supplement the maps with ongoing incident notifications and risk event tracking. So-called 'near miss reporting' will form part of monitoring throughout the year.

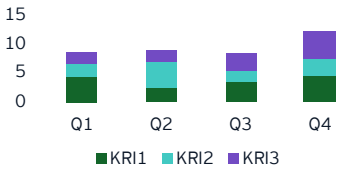
To facilitate the review process, many teams intend to prepare papers that bring together all the various reporting across the year into one summary overview. Furthermore, those that do not already do this are developing principal risk dashboards setting out a variety of information, including on the effectiveness of the related material controls alongside principal risk owner attestations. This can also be an opportunity to revisit whether definitions and material controls lists remain appropriate for the year ahead.

Example of dashboard content

- Risk description

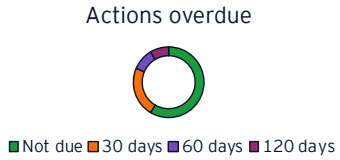
Sub-risk	Residual risk rating	Risk trend	Action

- Risk appetite statement



- Key metrics and risk indicators
- Near miss/incident reporting
- Compliance confirmations

- Risk owner and board-level oversight



- Second- and third-line activities
- External sources of assurance
- Underlying key control effectiveness
- Focus areas for next six months

- Material controls and observations on effectiveness criteria

- Overall assessment of residual risk by reference to risk appetite
- Risk/material control owner attestation

5.1.2 Timing

Provision 29 requires boards to monitor the risk management and internal control framework throughout the year and, at least once a year, carry out a review of the framework's effectiveness. The disclosable outcome of these board duties is that material controls are operating effectively. If not, boards must describe those material controls that have not operated effectively as at the balance sheet date, the action taken or proposed to improve them and any action taken to address previously reported issues.

Although the declaration is as at the balance sheet date, the review of the entire framework does not have to be performed exactly at year-end. Boards can instead align it to best fit in with existing meeting cycles and workloads and supplement it with monitoring activities to span between the date of the framework review and the material control declaration. This is the approach long taken by boards of investment trusts, which receive so-called System and Organization Controls (SOC) reports from their various providers at different times of the year, followed up with bridging letters at the year-end.

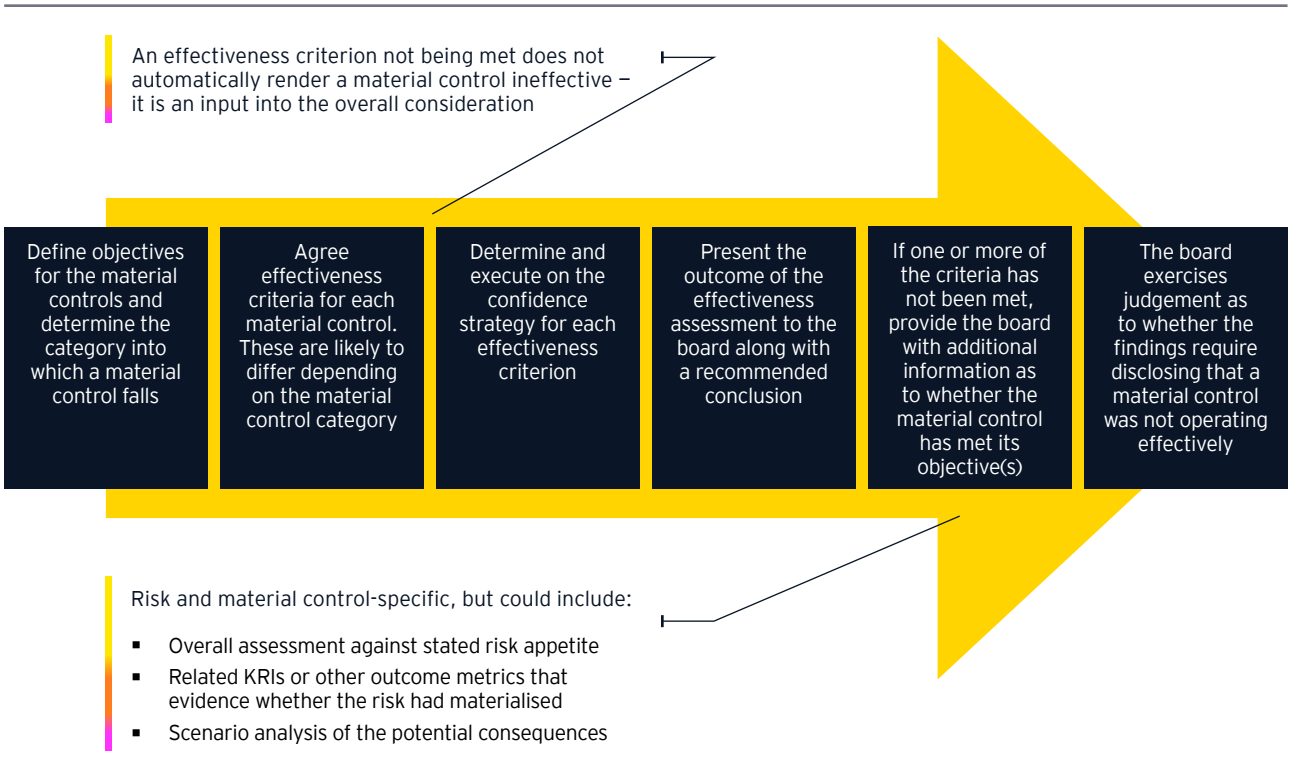
5.2 Making the declaration

The 2024 Code introduced a requirement to describe how the board has both monitored and reviewed the effectiveness of the risk management and internal control framework. We set out our formative views on addressing this requirement in our 2024 and 2025 publications dealing with Provision 29. We will provide updated examples based on 2025 reporting in our next ARA review publication. Our focus here is on the steps needed to make the effectiveness declaration itself.

5.2.1 Concluding on effectiveness

As explained in Section 3.2.2, effectiveness criteria serve as indicators that inform professional judgement rather than pass-or-fail tests. An effectiveness criterion not being met does not automatically render a material control ineffective, it is an input into the overall consideration. It is also important to acknowledge that the concept of operating effectively at a point in time is not as relevant for some categories of material controls or different types of risks they address as it is for others. While year-end effectiveness is well understood in the context of ICFR, this is very different for a health and safety single-risk framework. A lack of accidents on 31 December says very little about effectiveness – it's a single data point, and particularly meaningless if the majority of staff are on leave.

Following on from the considerations set out in 3.2.2 related to management's assessment, boards will need to form their own judgement. This will entail nuance and may require providing additional information to the board in the case of an effectiveness criterion not being met.



This information will be specific to each risk and material control, but could include:

- Overall assessment against stated risk appetite – this may require refocusing on how a company determines whether it remains within risk appetite
- Related key risk indicators (KRIs) or other outcome metrics that evidence whether the risk has materialised
- Scenario analysis of the potential consequences

5.2.2 Deciding whether issues require disclosure

A framework for deciding what should be disclosed as part of the declaration cannot be mechanical. It should consider the benefits of setting out issues, balance transparency with litigation and regulatory risk and consider matters that are already in the public domain. As one of the attendees of our roundtables put it: 'be transparent, not naked'.

Any issues that came to light as part of board monitoring during the year but were resolved by the year-end would not form part of the effectiveness declaration. In line with outcomes-based governance reporting under Principle C of the Code, directors may, however, choose to reference actions they had requested of management as part of the description of how they discharged their monitoring duty.[6]

Similarly, some may choose to flag areas of concern or those requiring further enhancements that were identified through the review process. For example, directors may wish to reference weaknesses in underlying key controls in a particular area, even if they did not lead to the conclusion that a material control was not effective as at the year-end.

If the board concludes that a particular material control was not effective as at the balance sheet date, the disclosure needs to:

- Describe the material control that was not effective. In some cases, simply referencing the risk that the material control was seeking to address achieves this most easily. For example, 'The material control over the health and safety risk did not operate effectively as at the balance sheet date'.
- Describe actions taken or proposed to improve it.

Many companies are concerned that such disclosures could be prejudicial or create an anchor for litigation against directors. Some foreign private issuers (FPIs) are already planning to exclude the declaration from their 20-F filing.

However, it is worth remembering that:

- There is no requirement to discuss the issues relating to the material control's effectiveness.
- When reporting on areas for improvement or actions that have been or are being taken, the board is not expected to provide any disclosures which in its professional judgment contain confidential information or any other information that could inadvertently affect the company's interests if publicly reported.[7]
- Even a major risk event occurring after the year-end does not immediately mean that a related material control had not been operating effectively. Controls over enterprise risks are not intended to fully eliminate them but rather keep them within risk appetite. There is, therefore, no equivalence between a subsequent restatement and what this implies about the effectiveness of financial reporting controls at year-end.

6 Governance reporting should focus on board decisions and their outcomes in the context of the company's strategy and objectives. (...)

7 Paragraph 299 of the guidance to the Code

6. Material controls over cyber risk: extended case study

Cyber risk dominates many of the Provision 29 conversations, with one roundtable participant aptly stating: 'cyber is ok, until it is not'. With high-profile attacks dominating the news in 2025, companies are wary of claiming effectiveness, only to fall victim to a major attack soon after. Many also see jeopardy in referencing weaknesses, lest they alert hostile actors to vulnerabilities, creating exposure.

Material controls over cyber risk exemplify the Goldilocks challenge. There is no one-size-fits-all approach as both the complexity of the risk and organisational maturity vary significantly.

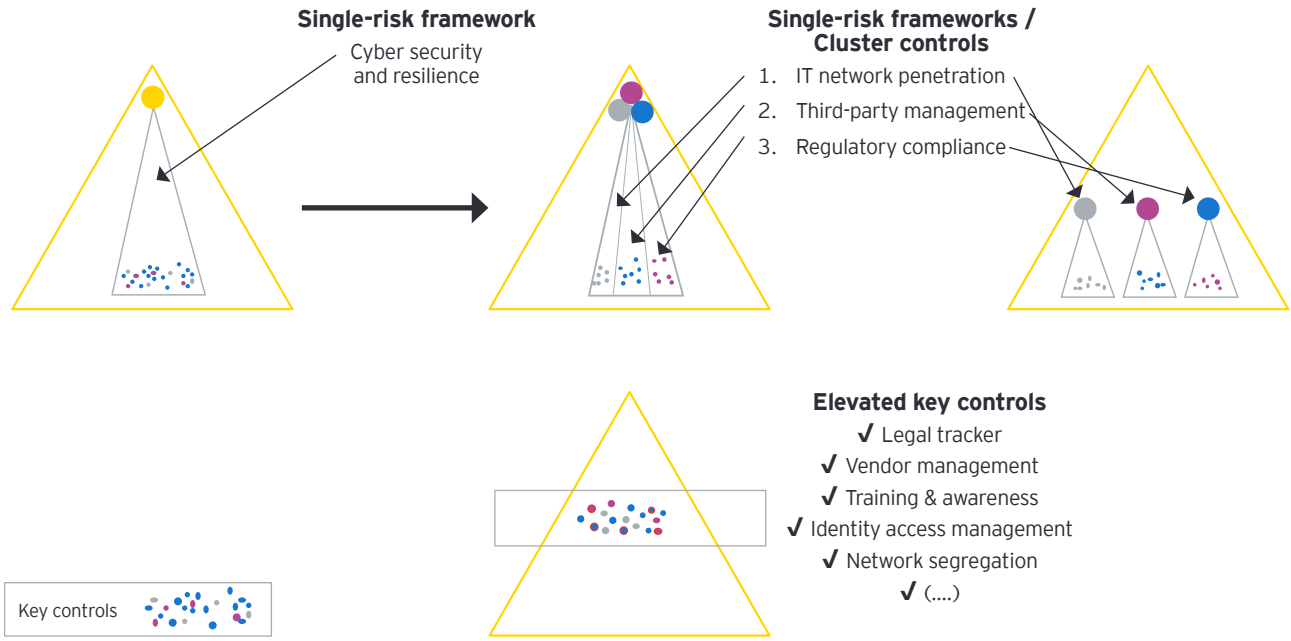
Some companies address cyber risk as a single-risk framework. Choosing a recognised approach such as the NIST CSF offers the additional option of obtaining an independent assessment against the standard, which can help identify gaps and provide an outside-in perspective on maturity. The NIST CSF is proving a popular choice. Although developed in the US, it is globally applicable, and aligns well with UK requirements, as its **mapping** to the UK Government's **Cyber Governance Code of Practice** demonstrates.

Others look at the tier below the principal risk, often differentiating between risks associated with their own network penetration and vulnerabilities associated with third party management. They treat these as cluster controls rather than frameworks to provide close oversight and monitoring from a cyber committee or forum.

In fact, some go a step further and look at the risk tier below, often elevating 'access management' to its own cluster.

Cyber risk – illustrative example[8]

▪ Principal Risk ▪ Tier 1	Cyber security and resilience						
▪ Key/material risks ▪ Tier 2	Regulatory compliance		IT network penetration			Third-party management	
▪ Sub-risks ▪ Tier 3	Sub-risk X	Regulatory non-compliance	Malware & Ransomware	Access Management	Data security	Access and change control	Cloud and infrastructure
▪ Key controls	Key control (...)	Key control (Regulation tracker)	Key control (Training)	Key control (Identity access management)	Key control (...)	Key control (Vendor management)	Key control (Vendor management)
	Key control (...)	Key control (Legal Register)	Key control (Network segregation)	Key control (Data security)	Key control (Data security)	Key control (...)	Key control (...)
	Key control (...)	Key control (...)	Key control (...)	Key control (...)	Key control (...)	Key control (...)	Key control (...)



For many organisations, the approach to cyber ends up being a pick-and-mix within the pick-and-mix model, with a different category of material control addressing the various sub-risks. Organisations address regulatory non-compliance through elevated key controls in the form of trackers or registers. They might treat third-party management as a single-risk framework. Cluster controls can be in place for each of the sub-risks within IT network penetration.

Application of Provision 29 to investee companies in a group context

The UK Corporate Governance Code applies to the entire group and under Provision 29, directors are required to 'monitor and review the risk management and internal control framework' of that group. If for financial reporting purposes something is classified as an investment, it is by definition 'outside the control' of the group. Directors are therefore not able to monitor and review the risk management and internal control framework of the investee company.

Risks to the group arising from investee companies should be considered as part of the risk identification process under Provision 28, with appropriate responses in place to address such risks, if relevant. If the risks are of such a magnitude that they can threaten the viability of the group or materially impact its share price, then some of those responses might be material controls.

8 This is an illustrative example of key risks and is not designed to be exhaustive.

Operational resilience as a material control in a cyber context

As highlighted in the *On Track* publication, in March 2021 the Prudential Regulation Authority (PRA) published Policy Statement PS6/21 ('Operational resilience: Impact tolerances for important business services'). The FCA published the equivalent PS21/3 ('Building operational resilience') at the same time. These set out rules to strengthen the operational resilience of banks, insurers and other in-scope firms and embed operational resilience into risk management and governance processes. Although aimed at financial services firms identifying important business services and setting impact tolerances for their maximum acceptable disruption, the concept of operational resilience is becoming more relevant to companies in the 'real economy'.[8]

Overview:

Organisations are now operating under sustained, high-frequency cyber threat conditions. Cyber incidents are no longer rare, containable technical events – they are business disruption events with financial, operational, regulatory and even systemic implications.

Over the past year there have been:

- Increasing attack severity and destructive impacts
- High profile supply chain and operational outages
- Regulatory tightening, with regulators treating cyber resilience as a national security issue

As a result, traditional prevent, detect and contain cyber controls, although necessary, are insufficient to manage the end to end harm path from a cyber event.

Assuming failure will occur

The biggest impact from severe cyber incidents arises after the breach, when companies struggle to continue delivering important business services. Companies that believe their prevent controls will be sufficient to stop disruption from occurring are mistaken. They miss out on low-probability, high-impact, black swan events, which if they were to occur would severely impact the organisation. This is why recent regulations have moved towards forcing firms to plan for 'severe but plausible' scenarios and require them to have recovery options that can help to deliver critical services while they recover from the disruption.

Given the threat environment and recent high-profile incidents, companies need to make the following baseline assumptions:

- Network penetration will occur
- The wider third-party ecosystem will immediately disconnect from affected organisations, even during a limited breach
- Third-party failures will flow through to the company
- Critical services will be degraded at some point

Operational resilience as a material control

Resilience is the ability to prevent, detect, respond, recover and learn from disruptions. Effective controls, therefore, need to span these areas and include what the firm does when failure occurs to maintain minimum service levels and avoid causing intolerable harm to clients, the market and the firm's own safety and soundness. The operational resilience framework needs to remain adequate, tested, resourced and governed. By adopting operational cyber resilience as a material control, organisations will confirm they have understood their critical services and impact tolerances, mapped the critical technology, people, premises and data required to deliver those services. They will have tested these to confirm they have options available to continue those services during disruptions.

A material control over the operational resilience framework could include:

a) **Design adequacy**

- Clear governance, ownership, and accountability for resilience
- Defined Important Business Services and impact tolerances/minimum viable enterprise
- Complete mapping of assets and third-party dependencies

b) **Scenario testing effectiveness**

- Regular, threat-led and cyber focused disruption scenarios
- Testing reversibility, recovery time and service continuity
- Evidence that vulnerabilities discovered through testing lead to remediation

c) **Monitoring and early warning capability**

- An integrated view of service health across technology, data, third parties and processes
- Proactive horizon scanning for cyber threats with business impact relevance

d) **Crisis management and recovery capability**

- The ability to transition from cyber response to business recovery
- Communication plans, decision support playbooks and executive-ready escalation

Summary

Cyber disruption is now expected, not exceptional. Identifying the operational resilience framework as a material control should provide confidence to directors that 'Even if our other cyber controls fail, our organisation can still remain within impact tolerances and continue delivering critical services'.

As regulatory expectations mature, e.g., the proposed Cyber Security and Resilience Bill in the UK; as technology evolves, including emerging threats for AI and quantum computing; and the shape of the organisation changes, the design of and confidence over this framework will require regular review and challenge.

– Jack Armstrong, Partner, Cyber & Resilience
jack.armstrong@uk.ey.com

8 Impact tolerance is the maximum tolerable level of disruption to an important business service as measured by a length of time in addition to any other relevant metrics.

7. Next practical steps

Based on our engagement, well-advanced companies have generally by now identified their material controls. They have categorised them and determined their effectiveness criteria. They have agreed on a confidence strategy with the board and are in the process of conducting a dry run to assess effectiveness.

Having navigated the Goldilocks phases of getting the fundamentals right: not too much, not too little, but just right for their circumstance, they are increasingly asking, 'So, what next?' Below is our view of some practical next steps.

1. Secure time on agendas – if the Provision 29 declaration requires additional activities from directors (for example, increased frequency of monitoring or time to consider proposed disclosures) – reflect this adequately in 2026/27 agenda planning.
2. Set aside time for post-dry run reflections and feedback. Consider doing a joint session with all risk owners, material control owners, or both to share learnings and streamline.
3. Start drafting summary review paper(s) to the board. Agree what it needs to include to be decision-useful for directors, without making it overly detailed and management oriented.
4. Prepare a draft disclosure setting out how the board monitored and reviewed the effectiveness of the risk management and internal control framework, based on the plans and intentions for 2026. Share it with directors as a means of pressure testing whether they are comfortable with the description of the degree of their involvement.
5. Pre-agree the basic text of the declaration, assuming all material controls are operating effectively. Then create a version where one material control was not effective. Given ongoing sensitivities, consider doing this for cybersecurity. Identify how such a disclosure would need to cross-refer back to other disclosures within the annual report.
6. Validate, with internal teams and directors, whether what was determined and agreed in 2025 in terms of material controls populations, their effectiveness criteria and confidence strategy remains valid for the year ahead.

But most importantly, organisations now need to focus on transitioning from a project mindset to lasting operational ownership and business as usual. The work done to define material controls, calibrate effectiveness criteria and establish confidence activities must be absorbed across the three lines and embedded into the wider risk culture. Sustaining this momentum will be essential to ensuring that the approach remains relevant as the organisation evolves and continues to support high quality board judgements. Keeping the understanding current through training and education – and ensuring it is lived rather than documented – will be critical to maintaining the discipline and proportionality that the Goldilocks phase is seeking to achieve.

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.

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

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

EYSCORE 000974-26-UK
ED None

UKC-042583.indd 02/26. Artwork by Creative UK.

ey.com/uk