PROTECHT

E-BOOK

How to prove control effectiveness with Provision 29.

What boards must do now to move from compliance on paper to assurance in practice.

protechtgroup.com

Executive summary

Provision 29 of the UK Corporate Governance Code marks a decisive shift in accountability. For the first time, boards must not only confirm that internal controls exist, but publicly declare their effectiveness. This raises the bar for oversight, risk management, and assurance.

What's changing

Board declaration: From 1 January 2026, annual reports must include a formal statement on the effectiveness of material controls. Therefore, the first wave of disclosures will appear in 2027 annual reports.

Beyond compliance: This is not a box-ticking exercise. The emphasis is on board-level accountability, judgement, and assurance.

Principles-based, not prescriptive: The FRC will not define "material controls" or prescribe wording. Boards must set their own approach. The FRC's guidance offers ways to think about materiality without defining it.

Scope: Mandatory for companies in the FCA's commercial category (previously premium listed); best-practice benchmark for others.

Key challenges

Ambiguity: No fixed definition of "material" risks or controls.

Stakeholder expectations: Pressure to balance comparability with company-specific approaches.

Control scoping: Boards are uncertain about how to scope controls in practice: how much they can group controls together and how many controls are sufficient.

What boards should do now

- Start early: Map your material controls and risk tiers now, not in late 2025. Build a quarterly cadence of evidence that accumulates toward year end.
- Define materiality: Apply judgement aligned to strategy, risk profile, and stakeholder expectations.
- Embed accountability: Ensure boards and committees are actively engaged, not just informed.
- Test and evidence: Move beyond risk registers; adopt structured testing and documented assurance.
- Communicate clearly: Prepare to explain your approach and effectiveness with confidence in the annual report.

How Protecht helps

Provision 29 is about moving from paperwork to proof. Protecht ERM equips boards and executives with the tools and evidence needed to meet the new declaration requirements:

- **Structured control library** aligned to COSO and ISO 31000.
- **Risk–control mapping** to show top-down alignment.
- **Automated testing workflows** and assurance templates for consistent evidence.
- **Real-time dashboards** for visibility of control effectiveness, issues, and remediation.
- **Auditable evidence** to support a confident board declaration.

We have also created a free checklist you can fill out and determine your readiness for Provision 29.

Download the checklist

View our solution

Contents

1 What is Provision 29?

It's one thing to have a fire alarm installed; it's another to prove it works when the smoke starts to rise. This need to replace potentially harmful assumptions with verification that an action has the desired result is being reflected in the corporate arena. For the first time, UK boards are being asked not only to confirm that internal controls exist, but publicly verify that they are effective.

Governance of internal controls is not a new concept. However, as the business risks, stakeholder expectations, and regulatory scrutiny evolve, the principles and standards that guide controls must evolve with them – otherwise they stagnate and fail. The latest revision of the 2018 UK Corporate Governance Code signals a decisive shift, raising the bar on expectations around risk, internal controls, and accountability.

At the heart of this change is Provision 29, which makes it clear that boards must seek additional clarity for their company's internal control environment to support the declaration of effectiveness.

Context: Why Provision 29 and why now?

The UK's renewed focus on internal controls did not emerge in a vacuum. It follows a series of high-profile corporate failures, most notably Carillion. which shook investor confidence and exposed weaknesses in board oversight. In the wake of these collapses, the UK Government consulted on introducing a US-style Sarbanes-Oxley (SOX) regime. Ultimately, that prescriptive approach was rejected.

Instead, the Government tasked the Financial Reporting Council (FRC) with developing a more flexible model that could strengthen accountability without creating a rigid compliance burden. Following consultation, the FRC revised Provision 29 of the UK Corporate Governance Code.

Several features of this revision are worth underlining:

- **Board accountability and oversight:** Provision 29 builds directly on the existing requirement for boards to review risk management and internal controls annually. The new element is the expectation that boards issue a formal declaration of effectiveness for material controls in their annual report.
- **Principles-based approach:** The FRC has deliberately avoided dictating what counts as "material" or prescribing the exact wording of declarations. That responsibility rests with boards, who must determine their own approach and be comfortable defending it.
- **Scope of application:** The Code applies to companies in the new FCA commercial category (previously premium listed). For these firms, Provision 29 is binding; for others, it serves as a governance best-practice benchmark.
- **Flexibility, not prescription:** By rejecting a SOX-style checklist, the FRC has signalled that the emphasis should be on thoughtful governance and board-level assurance, not a box-ticking exercise. Companies are expected to align the framework to their own size, scale, and complexity. However, dual listed issuers can leverage existing SOX frameworks rather than operate dual systems. This means if you're SOX compliant, you can reuse that framework for Provision 29.

Taken together, these changes shift responsibility for confirming the effectiveness of internal controls clearly to the boardroom. The FRC's stance is that it is not a regulator's role to define materiality or dictate disclosure formats – it is for each company to demonstrate that its board has exercised genuine judgement and accountability in making its declaration.

2 What does Provision 29 really mean for internal controls?

Under the Code, boards are already expected to monitor the company's risk management system and internal control framework, and to review their effectiveness at least annually. However, until now, there has been no explicit requirement to explain how this has been done or to declare whether controls are working.

Provision 29 addresses this by placing responsibility squarely on boards to ensure controls are not only in place, but effective, transparent, and responsive to evolving risks: "The board should monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness and report on that review in the annual report."

Starting 1 January 2026, boards must ensure their monitoring and review processes cover all material controls – including financial, operational, reporting, and compliance controls.

In the annual report, boards must now provide:

- A description of how the board has monitored and reviewed the effectiveness of the framework.
- A declaration of the effectiveness of the material controls as at the balance sheet date.
- 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.For companies on the London Stock Exchange, this is mandatory. For everyone else, it's a best-practice benchmark, providing a clear roadmap to stronger governance, greater resilience, and competitive advantage.

Provision 29 shifts responsibility for confirming the effectiveness of internal controls clearly to the top, not just to management or internal audit teams.

Think of it like piloting an aircraft. The engineers may have serviced the plane and checked every bolt and system, but before take-off, it's the captain's responsibility to run final checks and give the final go-ahead. A board's role under Provision 29 is no different. They must ensure the controls are not only implemented, but operational and effective before entering a new financial year.

With boards expected to actively review, assess, and report on how well internal controls are functioning, Provision 29 provides an opportunity for companies to 'get their house in order'. Rather than conducting a box-ticking exercise that lacks strategic value.

When put into practice, Provision 29 aims to elevate the management of internal controls in several ways:

- **Accountability:** With accountability placed on senior leadership, internal controls don't remain the responsibility of risk and compliance teams down the chain.
- **Risk management integration:** Internal controls are integrated with risk management, ensuring risks are identified and mitigated effectively.
- **Documentation and testing:** Internal controls evolve with the business and continue to be effective, backed by clear documentation and regular testing on a quarterly cadence building toward year end.
- **Reporting:** Control effectiveness is clearly disclosed, with any deficiencies promptly addressed through documented remediation plans and reported concisely at governance level.
- **Continuous improvement:** Internal controls are regularly reviewed and refined to keep pace with new risks, technologies, and regulations – rather than leaving them to stagnate.
- **Acceptable grouping:** Boards may group lower level controls into higher level material control themes where this better reflects how risk is managed—provided grouping remains monitorable and testable.

[1] EY: 2024 UK Corporate Governance Code
[2] PwC: Material Controls declaration under Provision 29 of the UK Corporate Governance Code

3 Comply or explain: what boards actually want.

Boards are demanding a change in focus from a compliance-first mindset to more strategic engagements with internal controls and risk management that underpin informed decisions.

They recognise that just meeting minimum governance requirements to satisfy regulators doesn't benefit the business; it exposes them to potentially crippling pitfalls – including:

- **Misplaced assurance:** A tick-box mentality can create the false impression that risks and controls are well-managed amid superficial documentation or minimum disclosures. When in fact risks are evolving and poorly understood, preventing controls from working in practice.
- **Inadequate risk management:** Compliance-focused processes typically treat risk as a static checklist rather than a dynamic, strategic imperative. This can lead to blind spots, where emerging or systemic risks, such as cybersecurity or ESG, aren't properly addressed.
- **Weak internal controls:** Controls implemented to simply comply typically lack robustness, integration, and employee engagement. These narrow controls may fail under pressure, exposing the company to operational or reputational damage.
- **Strategic value barrier:** When governance is seen as an obligation rather than a tool, boards are discouraged from engaging with risk and control frameworks to drive performance, resilience, and innovation.
- **Limited board insight and oversight:** Boards rely on surface-level assurance, clouding their view of what's really happening in the business. This undermines accountability and limits their ability to challenge ineffective controls.

Empowered by this broader perspective, boards are now seeking:

- Clarity around status of most important controls
- Digestible controls reporting to make informed decisions on where investment is required in the control environment
- Assurance that risks are being actively managed, not just documented
- Control opinions from 1st , 2nd and 3rd line of defence, and in some cases, external independent assurance

Provision 29 aligns with this quest for frameworks that work in practice, not just on paper. It outlines expectations to implement control assurance programmes that correspond with size, scale and complexity of the organisation. The result: boards can improve their accountability, enhance stakeholder confidence in internal control systems, and encourage a culture of continuous improvement – and ultimately gain confidence in their controls.

4 From risk registers to real assurance.

Traditional risk registers serve a purpose: they list identified risks, assign scores, and outline planned mitigation. But while they help organisations identify, analyse and mitigate risk, these static lists lack the evidence and verification needed to foster governance maturity. Consequently, they don't provide credible, board-level assurance that risks are being actively managed through effective internal controls.

Risk registers are inherently descriptive, not evidential. They list risks, scores, and planned actions without providing proof that controls are working as intended. Boards require assurance based on verification rather than declaration, yet risk registers simply show controls in place without demonstrating they have been tested, reviewed, or proven effective. As a result, they provide little indication that risks are being actively managed over time, functioning more as snapshots than a dynamic risk management tool.

This need for real assurance signals a shift from passively listing risks to actively demonstrating and declaring they're effectively managed by impactful, assessed controls, with board-level confidence. This translates into an approach where boards don't just see risks; they see evidence of whether controls are working – and formally report on it.

Provision 29 elevates risk management from paperwork to proof. It requires boards to be responsible – and publicly accountable – for the effectiveness of controls over material (or principal) risks, not just their existence. This evidence-based, documented review of the effectiveness of risk management and internal control systems strengthens accountability, supports informed decision-making, and reassures stakeholders.

PROTECHT

5 First-hand perspectives from industry leaders.

Whether your organisation is legally required to comply with Provision 29 or simply using it as a benchmark for governance maturity, the time to start turning what's on paper into practice is already here.

While Provision 29 applies formally to companies in the FCA's commercial category, its principles – especially around governance, accountability, and risk oversight – make it a strategic choice for companies outside its regulatory reach. Think of them as a safety-conscious cyclist in the Netherlands who, unlike a driver, isn't legally obliged to stop at red traffic lights, but chooses to for their own safety.

To understand why they're choosing to adopt Provision 29, how they're meeting its requirements, and the challenges they face, we spoke directly with industry practitioners.

Why?

Companies are choosing to align with Provision 29 voluntarily to demonstrate governance maturity.

- "We're aligning for best practice... not because we're obligated, but because we want to be the best function we can possibly be."
- "Aligning with Provision 29 is going to help us as a function show our maturity and then ultimately get the business's maturity up in those governance areas as well."

How?

Board and committee engagement

Board and committee engagement is the linchpin of Provision 29 progress. After all, it requires boards to take greater accountability for risk and control.

- "Provision 29 has shifted accountability to our board and committees, meaning they need to be engaged and genuinely interested in what's being reported. Through informal socialisation and collaborative feedback, we've built understanding and alignment before formal approval – creating a stronger foundation for meaningful oversight."

Risk tiering and materiality mapping

Using data-driven assessments to tier and map risks, companies are defining materiality at a strategic level.

- "We'd already thought that not all risks are equal... We were going through a process of tiering risks... then used that to identify our material risks."
- "It's already shifting the conversations. Everyone is talking about material risk."
- "We'd never looked at risk through this lens before."

Building confidence in internal controls

The process of building confidence in internal controls starts with first-line ownership and testing.

- "First line ownership is essential. That involves ensuring the people who own those controls have the training, the support, the capabilities to have their own self-assessment. And we have a programme of first-line control testing, so everything that's in our ERM platform goes through a testing schedule."

Challenges

As companies embark on their provision 29 journey towards a culture of greater board accountability and organisational transparency around risk and control, they are facing common hurdles, including:

Lack of definition in Provision 29

One recurring theme: ambiguity. Provision 29 doesn't define key terms like "material risk" or "material controls."

- "There's no definition of material risk. That was one of the first problems with provision 29. They just talk about material controls. They don't define material controls either, but that's what you need to report on. So, if we've got material controls what are they actually controlling?"

Different stakeholder expectations

From the level of detail required to balancing standardisation with flexibility, different stakeholders have different expectations.

- "People are concerned about a loss of detail... others are concerned this is introducing another layer of detail."
- "Some people want to do exactly what our peers are doing, but we're our own company. We might have similarities, but our risks are our risks, which then means our controls will be our controls."

Practical questions about scope

Boards and executives are also grappling with how far to take Provision 29 in practice:

- ***Can we group together some of our controls?*** Companies are asking whether it's acceptable to aggregate controls into higher-level themes to reduce complexity. The FRC has not prescribed a view here, but the underlying principle is clear: whatever grouping is chosen, boards must be confident they can stand behind a declaration of effectiveness. For example, grouping lower-level controls into a single material 'control theme' is fine if the board is confident it can monitor and test it. Oversimplifying could obscure weaknesses, while excessive granularity can overwhelm reporting.
- ***How many material controls should a company have?*** There is no "right" number. Some firms will identify a few dozen; others, several hundred. The test is whether the controls identified as material truly capture the risks that matter most to the business. Boards are expected to apply judgement rather than chase a numerical target.

Advice

Use Provision 29 as a maturity framework, even if your company's not mandated.

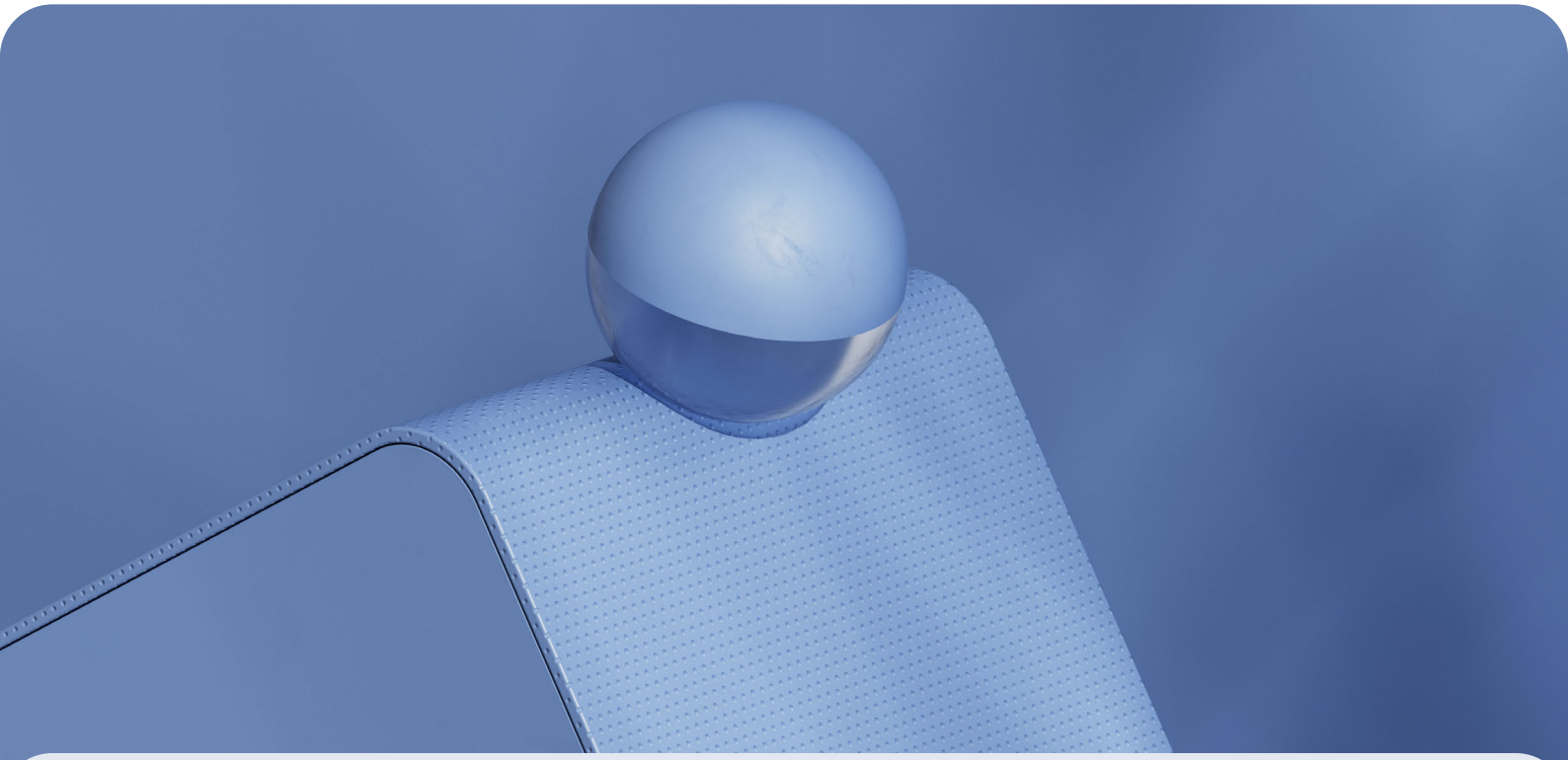
- "When you look at normal risk maturity frameworks, they're all a bit woolly and not very practical, but if you align with Provision 29, you start hitting those other maturity models. So, if you don't have to do it, my advice would be to still do it."

Start with the Protecht Provision 29 internal controls maturity checklist.

- "My biggest piece of advice is to use Protecht's structured checklist at the start."

Data-led validation of risk scoring is essential.

- "If we'd started with a data-driven analysis of our risks, we could be a couple more quarters ahead than we are now."



ABOUT PROTECHT

Redefining the way the world thinks about risk.

While others fear risk, we embrace it. For over 20 years, Protecht has redefined the way people think about risk. We enable smarter risk taking by our customers to drive their resilience and sustainable success.

We help you increase performance through better understanding, monitoring and management of risk. We provide a complete solution of risk management, compliance, training and advisory services to businesses, regulators and governments across the world.

Our Protecht ERM SaaS platform lets you manage your risks in one place: risks, compliance, incidents, KRIs, vendor risk, IT and cyber risk, operational resilience, business continuity management, and more.

We're with you for your full risk journey. Let's transform the way you understand and manage your risk to create exciting opportunities for growth.

AUSTRALIA & ASIA PACIFIC

+61 2 8005 1265

EUROPE, THE MIDDLE EAST & AFRICA

+44 (0) 203 978 1360

NORTH AMERICA

+1 (833) 328 5471

Visit our website:
protechtgroup.com

Email us:
info@protechtgroup.com

EBOOK-AIRISK-GL-2025-1.0