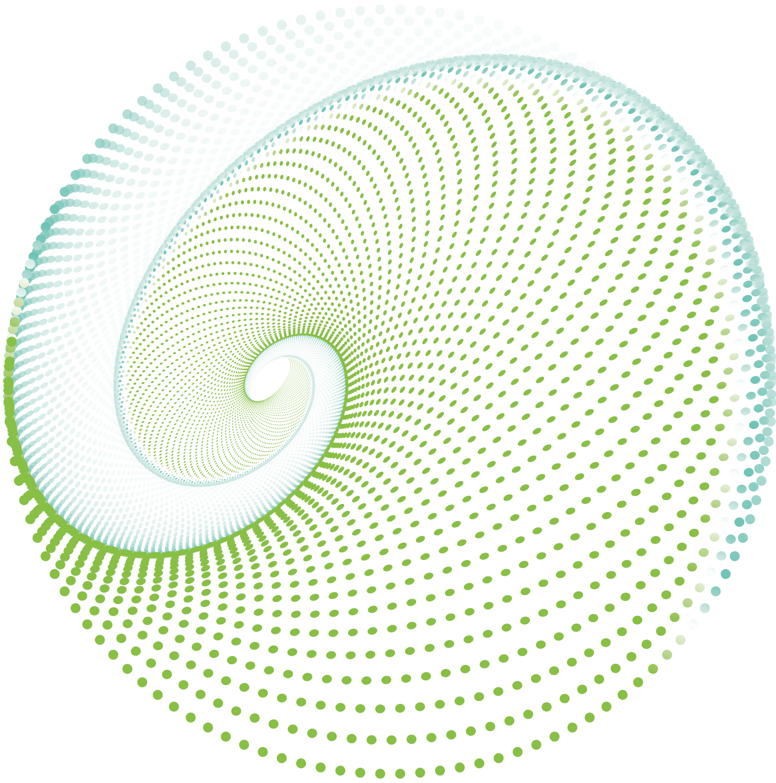
Deloitte.

The Deloitte Academy
April 2025



Risk, controls and assurance: a framework for the new material controls declaration

Introduction

In January 2024 the FRC issued an updated UK Corporate Governance Code ("the Code") which included changes to drive greater boardroom focus on the oversight of risk management and internal control matters.

The changes introduced are causing boards to reassess their current activities to ensure that they are appropriately robust to underpin the new expectations.

We issued the first edition of this publication in May 2024. We have now updated it to reflect insights gained from conversations and engagements over the past year.

With the ultimate aim of strengthening board accountability for the effectiveness of the risk and internal control framework, under the revised Provision 29 the board will be required to provide the following disclosure in the annual report:

- a description of how the board has monitored and reviewed the effectiveness of the [risk management and internal control] framework;
- a declaration of effectiveness of the material controls as at the balance sheet date; and
- 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.

The FRC believes that this new approach is a targeted, proportionate and balanced response to meeting enhanced investor and stakeholder expectations for better governance reporting around risk management and internal controls whilst minimising reporting burdens on businesses. The FRC also considers that this approach, which is principles based and relies on boards making their own judgements on what is material, is better suited to the UK commercial and governance framework than the more intrusive and prescriptive approaches required in some other jurisdictions.

Whilst the majority of the updated Code will apply to accounting periods commencing on or after 1 January 2025 there has been a carve out for the new Provision 29—the declaration on the effectiveness of the risk management and internal control framework—which will apply to accounting years commencing on or after 1 January 2026. Until then, existing Provision 29 of the 2018 UK Corporate Governance Code applies.

The updated Code is supported by newly issued guidance, the 2024 Code Guidance. The new guidance aims to bring together the most relevant content from previous publications into a single, condensed, digitally accessible and user-friendly resource. The FRC is keen to reiterate that the guidance is not part of the Code but a separate collection of information designed to help the application of the Code to different companies' needs.

In this publication, we set out:

- answers to a series of frequently asked questions (FAQs) to address many commonly held areas of misunderstanding and/or confusion;
- a suggested framework to approach the new disclosures;
- insights on determining the population of material controls;
- considerations on the nature of assurance;
- how to pull all the activity together; and
- a suggested structure for the new disclosures.

FAQs

In our conversations since the updated Code was launched, there are a number of common questions being asked. To help you and your boards, we felt it was important to start this publication with a "level set", answering and addressing many commonly held areas of misunderstanding and/or confusion.

We have grouped the FAQs into a series of different areas and have made clear where responses come from FRC source material [references in square brackets] or where they come from Deloitte SMEs.

The practicalities—scope, timing and impact on other governance codes

	FRC source material	Deloitte comment
Which types of companies does the Code apply to?	• The Code is applicable to companies listed in the commercial companies category or the closed-ended funds category (previously premium listed) on the London Stock Exchange, regardless of where they are incorporated. To comply with elements of the UK Listing Rules these companies must apply the Principles of the Code and comply with, or explain against, the Provisions. [FRC Code homepage]	• That means that it does **not** apply to companies in the transition category (previously standard listed), AIM quoted or large private companies unless they choose to voluntarily apply the Code. N.B. the FCA is planning to introduce changes to the Listing Regime later in 2024 which could bring some current companies in the transition category (previously standard listed) companies into a new Listing category which would need to apply the Code. • Previous discussion of a new definition of public interest entity (PIE) and/or 'large PIEs' is **not** relevant to application of the Code.
What is the date of implementation?	• The 2024 Corporate Governance Code will apply to financial years beginning on or after 1 January 2025. However, Provision 29 (the internal controls declaration) will apply one year later for financial years beginning on or after 1 January 2026. For that first year, Provision 29 of the 2018 Code continues to apply. [FRC 2024 Code]	• We recommend that boards use 2025 to conduct a 'dry run' of the processes to monitor and review the effectiveness of the risk management and internal control framework, including understanding sources of assurance, followed by developing a draft declaration

<table>
<tr><td rowspan="4">Will there be a transition period?</td><td>FRC source material</td></tr>
<tr><td>• The 2024 Code does not become effective until reporting years beginning on or after 1 January 2025. Therefore, there will not be a transition period. The FRC has explained that reporting will be dependent on the make-up of a company. The flexibility of both the principles and the ability to explain against the Code provisions offers newly listed companies an opportunity to report on their own unique circumstances.
[FRC webinar Q&A]</td></tr>
<tr><td>Deloitte comment</td></tr>
<tr><td>• The FRC has also made clear that it recognises that some aspects of control (e.g. controls over non-financial reporting) may be less mature and therefore not capable of full assurance of effectiveness for the purposes of the declaration. This could be another reason for a board deciding to report a non-compliance.</td></tr>
<tr><td rowspan="2">Impact on the Wates principles of corporate governance for large private companies</td><td>Deloitte comment</td></tr>
<tr><td>• There is no automatic mechanism for changes to the UK Code flowing through to the Wates principles.
• It is possible that the FRC may choose to review the principles at some point because they have not been re-visited since they were launched in December 2018.</td></tr>
<tr><td rowspan="2">Impact on the AIC Code</td><td>Deloitte comment</td></tr>
<tr><td>• An updated AIC Corporate Governance Code was issued in August 2024 to reflect the changes made to the UK Corporate Governance Code. Within that code Provision 34 is the internal controls provision and the following supplementary guidance has been provided: “What is a ‘material control’ is for each individual board to determine. Material controls will be company-specific and therefore different for every company depending on their features and circumstances, including, for example, the company’s size, maturity, complexity and strategic objectives. The needs for each company may vary. The approach boards take in relation to this Provision should be a targeted, proportionate and balanced response to meeting enhanced investor and stakeholder expectations for better governance reporting around risk management and internal controls whilst minimising reporting burdens on the company. The intention of the declaration is for boards to make a public statement about the work they already undertake on the effectiveness of material controls. There is no expectation that making this declaration will require any significant change to the processes or procedures that boards already perform”. [The AIC Corporate Governance Code]</td></tr>
</table>

Guidance for the 2024 Code

<table>
<tr><td rowspan="4">Does the 2024 guidance apply for the 2018 Code?</td><td>FRC source material</td></tr>
<tr><td>• The FRC has released new Guidance to support the 2024 Code. The purpose of this guidance is to support those who use the 2024 Code by providing advice, further detail and examples. The guidance is not intended to be prescriptive. [FRC Code homepage]</td></tr>
<tr><td>Deloitte comment</td></tr>
<tr><td>• For the 2018 Code, the existing guidance notes remain relevant: The Guidance on Board Effectiveness; The Guidance on Audit Committees; and The Guidance on Risk Management, Internal Controls and Related Financial and Business Reporting.</td></tr>
<tr><td rowspan="4">What is the status of the supporting guidance?</td><td>FRC source material</td></tr>
<tr><td>• The guidance is not mandatory, and not part of the Code itself, and is not prescriptive. It contains suggestions of good practice to support directors and their advisors in applying the Code. Where the term ‘must’ is used there is a direct reference to a specific, legislation, or rules. [Guidance para 3]</td></tr>
<tr><td>Deloitte comment</td></tr>
<tr><td>• The FRC is updating the guidance to indicate where material in the guidance is derived from the Code itself or other law or regulation. This is an ongoing process.</td></tr>
<tr><td rowspan="2">Was the Guidance consulted on?</td><td>Deloitte comment</td></tr>
<tr><td>• It was subject to review by the FRC’s Stakeholder Insights Group but there was no formal public consultation.</td></tr>
</table>

Enforcement

<table>
<tr><td rowspan="4">What enforcement takes place of the Code?</td><td>FRC source material</td></tr>
<tr><td>• The FRC monitors compliance with the UK Corporate Governance Code and publishes an annual review setting out good practice and areas for improvement. The Code is not associated with enforcement mechanisms such as sanctions or penalties. Investors should consider the disclosures and engage with the company on reporting that they have concerns with. The Code is underpinned by the Listing Rules and [the FCA] may wish to follow up should a company not report.
[FRC webinar Q&A]</td></tr>
<tr><td>Deloitte comment</td></tr>
<tr><td>• It is also worth noting that the FRC’s Corporate Reporting Review team has been reviewing corporate governance disclosures on a voluntary basis until such time as the Audit, Reporting & Governance Authority is established with the necessary powers to review on a more formal basis.</td></tr>
</table>

The controls declaration

Question	FRC source material / Deloitte comment
Is there (or will there be) an FRC benchmark for how the new declaration should be addressed and presented?	**FRC source material** • The FRC has said that it is not setting a benchmark. Annual reports are for investors and stakeholders and should be used as an opportunity for additional engagement. Investors will want to consider the declaration in terms of the company and seek assurance that the board has appropriate oversight of the risk and internal controls framework. The FRC will want to see that companies have reported on their monitoring and review, made a declaration of effectiveness of controls and described any controls that have not operated effectively. [FRC webinar Q&A] • The number of items disclosed is expected to be relatively small and should not result in a comprehensive list of performance measures or internal controls. [FRC webinar Q&A] **Deloitte comment** • In relation to the bullet above and the reference to "number of items", it is not our expectation that the declaration will provide a detailed list of the controls covered by the declaration, more that there will be an explanation of how the board has determined the population of material controls (see page 13 for the further suggestions in relation to the new disclosures).
What should be included as a material control?	**FRC source material** • While the board decides which controls are material these could include, but are not limited to, controls over: • risks that could threaten the company's business model, future performance, solvency or liquidity and reputation (i.e. principal risks). • external reporting (financial or non-financial) that is price sensitive or that could lead investors to make investment decisions, whether in the company or otherwise. • fraud, including override of controls. • information and technology risks including cybersecurity, data protection and new technologies (e.g. artificial intelligence). [FRC Guidance para 272] **Deloitte comment** • Please see the section 'How to determine the population of material controls' starting on page 8.
Should the board be explaining its approach to determining material controls?	**Deloitte comment** • We recommend that this transparency is provided so that stakeholders are clear on the context for the declaration. • As investors have expressed real interest in how boards reach their judgement on the effectiveness of controls, this is expected to be an area of attention for governance teams at investment houses.
What is expected to be covered in the category of "reporting controls"?	**FRC source material** • Reporting controls include those which cover the non-financial report in the annual report and accounts, and those reports that could impact on investor confidence, if considered material by the board. When determining which controls are 'material', the board considers how a deficiency in the control could impact the interests of the company, shareholders and other stakeholders. [FRC webinar Q&A] • Provision 29 of the 2018 Code already required that boards monitor, review and report on financial, operational and controls. The 2024 Code asks that the board make a declaration of effectiveness over these controls and extends these controls to include those over reporting, such as narrative and ESG reporting controls. [FRC Code homepage] • Material controls may take many forms – the change is to recognise that for some companies reporting on either financial or non-financial controls may be significant and therefore should be included within the review. [FRC webinar Q&A] **Deloitte comment** • It is worth noting that existing Principle M of the 2018 Code states the following: "The board should establish formal and transparent policies and procedures to [.......] satisfy itself on the integrity of financial and narrative statements". This is supported by a footnote which says that the boards' responsibilities here "extends to interim and other price-sensitive public records and reports to regulators, as well as to information required to be presented by statutory instruments". [FRC 2018 Code]
Will boards have to seek assurance over controls?	**FRC source material** • It will be for boards to decide the level of internal or external assurance which they wish to seek in relation to their declaration on internal controls. External auditors have a role to play in considering the disclosures within the annual report, there is no change to this. [FRC webinar Q&A] **Deloitte comment** • In relation to assurance, we recommend that companies look again at the assurance mapping activities that many had started in preparation for the Audit & Assurance Policy as this should help the board to understand, and plan for, assurance needs across controls and reporting in order to make the new declaration. For further discussion on assurance please see pages 10 to 11.
What is the role of internal audit?	**FRC source material** • The Code does not require sign-off by other internal or external parties of the declaration made by boards. Boards themselves will decide on the level of assurance required, and on the publication of assurance materials. [FRC webinar Q&A]

If a weakness or failing in a control has been fixed by the year end does it need to be disclosed?	**FRC source material** • The material controls which need to be disclosed as part of the declaration are those which are not operating effectively at the balance sheet date. However, if a failure had been reported to the market during the year it would seem appropriate to cover this at the end of the year. [FRC webinar Q&A]
Would all matters reported as a significant deficiency by the auditors to those charged with governance (under ISA (UK) 700) be reportable under the third bullet in Code Provision 29?	**Deloitte comment** • The provision refers to reporting of material controls that have not operated effectively as at the balance sheet date, so will depend on the deficiency and whether it is deemed (by the board) to relate to a material control (the same is true for material weaknesses reported under Sarbanes-Oxley although it is probably likely that there will be more alignment of scope in this regard). This reinforces the importance of providing a clear explanation of what the board has deemed to be a material control so that stakeholders have visibility and can understand the differences.
Although the declaration is about effectiveness as at the balance sheet date, presumably this will be based on routine/regular testing throughout the year and, where necessary, the period up to the signing of the annual report?	**FRC source material** • The declaration covers information collected before and on the date of the balance sheet. There may be further procedures that are necessary for the company to carry out as part of its internal controls framework, which occur after the date of the balance sheet, and may be relevant to making a declaration on the effectiveness of the framework. [Guidance para 300]
If we are already using an internal controls framework such as COSO, are we allowed to continue with that?	**FRC source material** • The board could use a recognised framework or standard as part of its process for designing and maintaining the effectiveness of the risk management and internal control framework (e.g. COSO, ISO, COBIT, etc.). Such framework or standard should be relevant for those areas which it relates to (e.g. financial reporting, technology, etc.) when reporting against the Principles and Provisions of the Code. [Guidance para 217]
Is there a seriously prejudicial type exemption from disclosing certain control failings?	**FRC source material** • 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 judgement contain confidential information or any other information that could inadvertently affect the company's interests if publicly reported. [Guidance para 299]
What would you expect a non-compliance with Code Provision 29 to look like?	**Deloitte comment** • Code Provision 29 requires the board to monitor and review the company's risk management and internal control framework and to provide the required disclosures. The presence of any ineffective material controls would NOT be a non-compliance as long as the review and monitoring has taken place and suitable disclosures have been provided. • It is expected that the disclosures around Code Provision 29 will include an explanation of the approach adopted to support the board making the declaration. The presence of such an explanation is not an indication of non-compliance. The FRC has gone to great lengths not to specify a particular approach, encouraging boards to "think for themselves". So we do not expect anyone to have to report a non-compliance based solely on the approach they have taken as long as explained clearly and reasonable. • Reporting a non-compliance should only be necessary in a situation where it has not been possible to reach a conclusion on the effectiveness of a particular element of the material controls.
Will this end up being more boilerplate statements?	**FRC source material** • It is directors that need to take the lead and ensure that the company is reporting effectively on its governance arrangements in a way that is relevant and beneficial to the users of their reporting. Directors should focus on practices, as opposed to policies and procedures, to demonstrate that a company is well governed, sustainable and able to deliver investment, growth and competitiveness. [FRC mythbuster]
What documentation will be required?	**FRC source material** • 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. [FRC Guidance para 278]
Will companies use 2025 to do a dry run of the declaration?	**Deloitte comment** • Our expectation is that companies will use the 2025 financial year to finalise their population of material controls, to identify the sources of assurance over the effectiveness of those controls and to dry run the testing and documentation process through to a draft declaration. We are recommending that companies involve their auditors in this dry run process to allow early discussion of the approach.

Integrated Risk Management & Control Framework—line of sight through risk, control and assurance

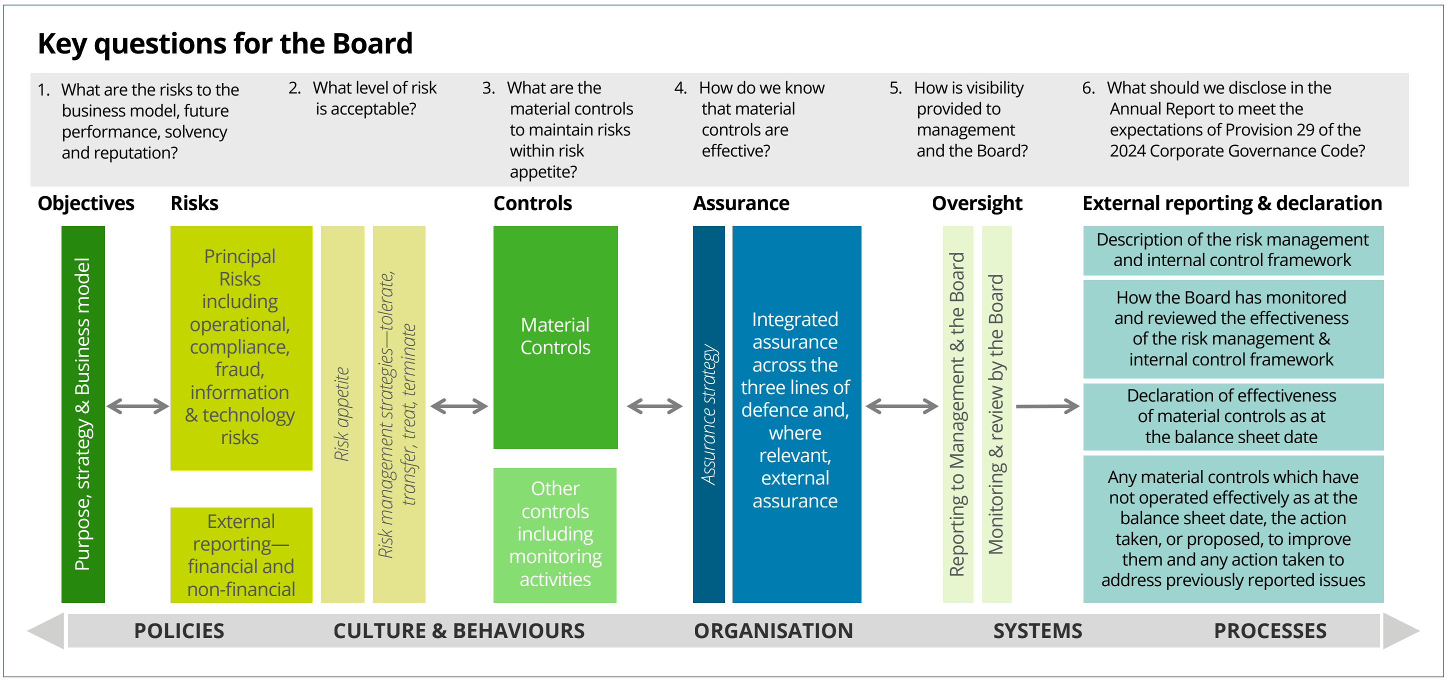
The ultimate aim of these changes has been to strengthen board accountability for the effectiveness of the risk and internal control framework. In addition to the change to Code Provision 29, and to underpin this focus on board accountability, there has been a small but significant change to the relevant Code Principle: "The board should establish a framework of prudent and effective controls, which enable risk to be assessed and managed" is replaced by "The board should establish **and maintain** an effective risk management and internal control framework". The addition of a responsibility for maintaining an effective risk management and internal control framework provides a clear foundation for the new declaration in terms of the board's oversight and visibility of the effectiveness of the design, implementation and operation of the risk management and internal control framework.

While the new Code Provision 29 applies for periods commencing on or after 1 January 2026, this new principle applies for periods commencing on or after 1 January 2025. This means that the disclosures explaining how the Code principles have been applied during 2025 will need to reflect this extension to the old principle.

The new 2024 Code Guidance sets out matters for boards to consider in meeting their responsibilities—we highlight some key elements here:

- Procedures and processes should be in place to determine **the amount of risk that a company is willing to accept** in pursuit of its strategic objectives (risk appetite). [para 239]
- The board should establish the extent to which principal risks are to be managed or mitigated, and which controls will be put in place. Controls implemented should be appropriate to **maintain these risks within the defined risk appetite**. [para 250]
- 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. [para 263]
- The board could use a **recognised framework or standard** as part of its process for **designing and maintaining** the effectiveness of the risk management and internal control framework (e.g. COSO, ISO, COBIT, etc.). [para 217]
- Material controls will be **company-specific** and therefore **different for every company** depending on their features and circumstances, including for example size, business model, strategy, operations, structure and complexity. [para 270]
- When determining which controls are 'material', the board considers how a deficiency in the control could **impact the interests of the company, shareholders and other stakeholders**. [para 271]
- There is **no requirement or expectation** in the Code or this guidance that companies obtain **external advice or assurance** over the effectiveness of the material controls. It may not be necessary for a company to do so, particularly when it has an effective internal audit function that is appropriately resourced to provide assurance over the effectiveness of the framework. [para 274]
- 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. [para 294]

From the guidance and our own experience, we have developed the framework below as a way of developing a clear line of sight through risk, control and assurance—starting with the organisation's purpose, strategy and business model and ending with the board's declaration and other reporting. The framework highlights key questions that boards need to be asking for each stage.



Key to achieving a proportionate and practical response to the new declaration, is the identification of "material controls". The Code states that "material controls" should include "financial, operational, reporting and compliance". The inclusion of a specific "reporting" control consideration is intended to cover controls over both financial and non-financial reporting. The FRC press notice accompanying the release of the updated Code states that it is for a board to determine what should comprise its material internal controls, noting that the needs for each business may vary.

How to determine the population of material controls

As a starting point, and as included in our FAQs section, the FRC has provided the following guidance (FRC Guidance para 272) which suggests that material controls could include controls over:

- risks that could threaten the company's business model, future performance, solvency or liquidity and reputation (i.e. principal risks);
- external reporting that is price sensitive or that could lead investors to make investment decisions, whether in the company or otherwise;
- fraud, including override of controls; and
- information and technology risks including cybersecurity, data protection and new technologies (e.g. artificial intelligence).

In our opinion, as depicted in the framework set out in the previous section, there are two clear starting points for determining material controls: the principal risks and the processes for external reporting.

Principal risks

Principal risks are defined in the Code as including, but not necessarily limited to, those risks that could result in events or circumstances that might threaten the company's business model, future performance, solvency or liquidity and reputation. Companies have been disclosing their principal risks in the Strategic Report for many years and these disclosures are also required to include a description of the way those risks are being managed and/or mitigated.

We have heard from many organisations that this exercise to determine the population of material controls has started with a re-examination of the principal risks. The new declaration is focusing attention not just on what the principal risks are but also the way they are described and whether that a) can be easily reconciled to the group risk register and b) is sufficiently specific to identify a corresponding control or set of controls.

A workshop with senior leadership, key functional stakeholders and risk and controls experts can be an effective mechanism for re-examining the principal risks. Each principal risk is analysed and, where necessary, broken into sub-risks, with the aim of identifying the core element(s) of the principal risks which are subject to a control.

Not all principal risks are able to be 'controlled', for some risks, e.g. geopolitical type risks, the 'control' will involve monitoring activity. It is also true that for some risks, there will not be a one-to-one alignment of a risk to a control and it will be more appropriate to identify an overarching framework of controls which ensures that a principal risk is managed effectively. Our expectation is that the population of material controls will consist of a combination of stand-alone controls and framework controls.

This is a key stage for input and challenge from the risk and control experts within an organisation to ensure that the articulation of the control is appropriate and that the control is documented, will be able to be tested and with evidence of the outcome available. Getting the right people in the room at this stage is important. In our experience, bringing together the CFO, the CRO (where there is one) and the Head of Internal Audit helps to drive effective considerations.

Processes for external reporting

External reporting comprises two clear elements: financial and non-financial. The FRC Guidance suggests that the material controls in this area should focus on external reporting (financial and non-financial) that is price sensitive or that could lead investors to make investment decisions in relation to the company.

This is another area where we have seen framework controls being identified as the 'material control'. For example, for SEC registrants reporting under the Sarbanes-Oxley Act, the framework adopted to allow the organisation to make the SOx attestation[1] could be deemed to represent one material control.

1 See Appendix for an explanation of the difference between the Code approach and the US approach under Sarbanes-Oxley

Governance arrangements

In our experience, it is the audit committee which is the board entry point for management to test and agree the proposed approach to the new Provision 29 including the determination of the population of material controls. For calendar year end companies, we saw papers setting out the initial approach shared with audit committees in Q4 of 2024. Our expectation is that management teams will be reflecting on feedback received and further refining the population during the first half of 2025.

Whilst we agree that it is appropriate for the audit committee to be taking the lead in these discussions, we would urge audit committees to keep the rest of the board fully aware of the decisions being taken. This is a full board declaration and all board members will need to be comfortable that the material controls have been identified appropriately.

It is also recommended to have early discussions with the external auditors on the process. Whilst no specific statutory auditor requirements have been issued, existing auditor responsibilities for reviewing “other information” in the annual report will apply. Specifically this means that the auditors will be required to confirm in their audit report that the disclosures in relation to Provision 29 (including the new declaration) are materially consistent with the knowledge obtained through the audit.

This consistency point could come into focus in relation to any controls over financial reporting included within the population of material controls as the auditor is likely to have assessed those controls as part of their audit procedures and so will have a view on their effectiveness (which they may or may not choose to discuss in the auditor’s report). In addition, the auditor will likely want to see evidence of any process described within the disclosures.

Compliance

We stress that whilst we are trying to share insights on how to determine the population of material controls based on what we have heard from a number of different organisations, there is no right or wrong way to approach this as long as a clear process is established which can be explained to stakeholders. On this basis, and the fact that the FRC has repeatedly told boards that they should “think for themselves”, we would not expect a non-compliance with the Code to be disclosed in relation to how material controls have been determined. As noted on page 5, reporting a non-compliance should only be necessary in a situation where it has not been possible to reach a conclusion on the effectiveness of a particular element of the material controls.

Assurance

With the population of "material controls" established, boards can then move to a conversation about the nature and extent of testing and assurance they wish to put in place to allow them to reach the judgement on effectiveness for the new declaration and the supporting evidence and documentation they require. The FRC has made clear that it is for the board to determine the nature and level of assurance obtained in relation to the effectiveness of these controls.

Documenting and evidencing the effectiveness of the material controls is a key step in preparing for the new declaration and involves close collaboration with business stakeholders to create documentation that captures the essence of each material control and its supporting evidence. Identifying appropriate owners for each material control drives clear accountability for the design, operation and effectiveness of each material control and contributes to the overall assurance.

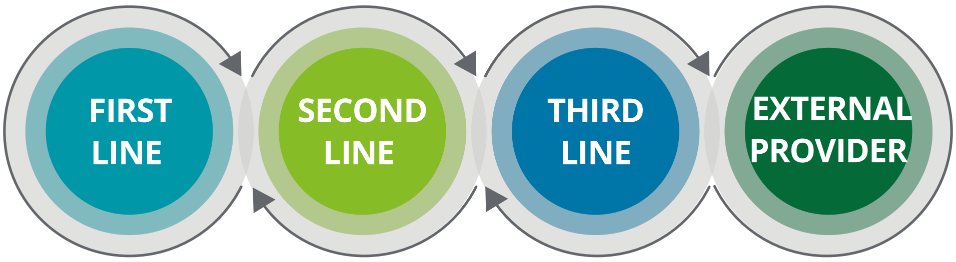
How to determine whether a control has operated effectively

A key step is to agree what "effectiveness" means. The FRC Guidance (para 286) makes the point that when a control is said to be effective that "does not mean that the risk is eliminated". An effective control should be working to keep an identified risk within the board's agreed risk appetite.

In addition, an indicator of where a control has been **ineffective** could be where there has been a material misstatement in any external reporting that is price sensitive or that could lead investors to make investment decisions.

Who is providing assurance?

Assurance is a complex area, with different levels of assurance offering different levels of confidence to stakeholders from both internal and external sources. The diagram below considers where assurance can come from:



INTERNAL/EXTERNAL ASSURANCE	
• Assurance under ISAE 3000 (Revised) should only be provided by a suitably qualified, independent assurance practitioner and is for use by the Board/Audit Committees, 3rd party stakeholders and other users of the subject matter information • Effective use of internal lines of defence can go some way in providing confidence to the board and internal stakeholders over the information that is reported and any associated business model risks, and it may be appropriate for some elements of assurance reporting, depending on the complexity, risk and levels of confidence required by stakeholders • External, independent assurance and provision of a formal opinion gives users the greatest degree of confidence in the subject matter where subject matter and processes are sufficiently mature and of particular importance to stakeholders	
FIRST LINE	**SECOND LINE**
• Managers and staff who are responsible for identifying and managing risks as part of their accountability for achieving objectives • Collectively, they should have the necessary skills, information and authority to operate the relevant policies and procedures of risk and control	• Internal functions that oversee or specialise in assuring compliance and risk management procedures in the first line • They provide policies, frameworks, and support to enable risk and compliance to be managed, monitor the effectiveness of this, and help to ensure consistent definition and management
THIRD LINE	**EXTERNAL PROVIDER**
• Provided by internal audit—its main roles are to ensure that the first two lines are operating effectively and to provide independent, periodic monitoring and recommendations on their controls	• Independent assurance—provided by an external party, under standards-based assurance, which provides more objective and challenging levels of assurance and a formal opinion

As part of the preparations for the, now withdrawn, requirement for an Audit & Assurance Policy, many companies will have started an assurance mapping exercise to build an understanding of where different sources of assurance were obtained in relation to external reporting. To help boards prepare for the new material controls declaration, it would seem sensible to extend this mapping, if it hadn't already, to also cover assurance over the effective operation of material controls beyond external reporting, e.g. material financial, operational and compliance controls. That way a full picture of assurance (from all sources – both internal and external) can be developed and assessed and any gaps identified.

Understanding external assurance options

For external assurance engagements the terms limited and reasonable assurance are often used, but there is often a lack of clarity of what those expressions mean, and difficulty in articulating the differences to stakeholders. The FRC provides a definition in its Glossary of terms, but the differences are summarised in the table below:

	LIMITED ASSURANCE	REASONABLE ASSURANCE
Definition	• The practitioner collects evidence sufficient for a negative form of expression of the practitioner's conclusion. The practitioner achieves this ordinarily by performing different or fewer tests than those necessary to form a reasonable assurance opinion. For both limited and reasonable assurance, evaluation of the subject matter vs clear criteria is fundamental.	• The practitioner needs to reduce the assurance engagement risk (the risk that an inappropriate conclusion is expressed on the information on the subject matter) to an acceptably low level as the basis for a positive form of expression of the practitioner's opinion
Opinion wording example	• "Based on the procedures performed, nothing came to our attention to indicate that the management assertion on XYZ is materially misstated."	• "Based on the procedures performed, in our opinion, the management assertion on XYZ is reasonably stated."
Features	• Procedures performed in providing the opinion are less extensive • Less cost for the engaging party • Less risk for the practitioner potentially • Provides users with a lower level of comfort as to whether the subject matter is materially misstated • Well suited for clients where control procedures are less mature and less well-embedded in ongoing procedures	• May not be appropriate in some circumstances (e.g. less mature internal control environment) • Procedures performed in providing the opinion are more extensive • Higher cost for the engaging party • Higher risk for the practitioner potentially, not if controls are mature • Provides users with a higher level of comfort as to whether the subject matter is materially misstated
Example of types of procedures	• Testing relies more heavily on management inquiry and/or analytical procedures • Less detailed testing procedures (e.g. often limited to inquiry and observation) with a minimum of testing • Limited or no sampling - where sample sizes are used, these are typically less than those for reasonable assurance • Procedures performed may be focused only on certain areas rather than covering all material balances	• Testing procedures typically include a mix of inquiry, observation, inspection, confirmations, and re-performance • Sampling across all or most material areas with a higher number of sampled items • Robust risk assessment to determine the nature, timing, extent and consideration or procedures • Reporting is more appropriate for stakeholders in higher risk assurance areas, like ESG and fraud

When deciding whether to obtain external assurance, it is important to consider whether a process is ready to be subject to such an assessment. For example, as ESG reporting processes mature, an "assurance readiness assessment" and gap analysis can help companies understand how they measure up against frameworks in terms of disclosure, where improvements can be made, and how processes can be more effective. A readiness assessment helps ensure the investment in an assurance opinion comes at the right time, avoiding unnecessary adverse findings and providing constructive challenge and recommendations in the meantime.

Pulling it all together

Building on the previous stages, establishing a robust and comprehensive reporting process is crucial for supporting the attestation and ultimately the new Provision 29 declaration. A structured process should help to ensure the accuracy and completeness of information feeding into the declaration and align with the overarching objectives of the Provision 29 compliance journey.

While many organisations leverage existing Governance, Risk, and Compliance (GRC) platforms and tools, some opt to develop separate processes and toolkits for closer monitoring and more efficient reporting. Regardless of the chosen approach, a thorough assessment of the reporting process is essential and should consider the end-to-end flow of information, from data capture to declaration.

Key aspects to consider include:

- **Governance structures:** Define clear roles and responsibilities for data collection, validation, reporting and review.
- **Documented guidance:** Ensure readily accessible and comprehensive guidance is available, including control narratives and any relevant policies or procedures.
- **Data inputs:** Determine the specific data required for reporting and assess whether existing systems and reports can provide this information. Identify any need for custom report development.
- **Maintenance and monitoring:** Establish procedures for ongoing maintenance and monitoring of the reporting process to ensure data quality, timeliness of controls assurance activities that enable timely identification of any emerging issues.

Positive behaviours we have observed

Senior sponsorship

A key differentiator for successful programmes is the commitment from senior leadership, including executives and board members. Where this goes beyond endorsement and includes active involvement and advocacy it demonstrates the significance of the exercise and fosters a risk and controls aware culture. Leaders in these organisations champion the process, ensuring adequate resources are allocated and that the "tone at the top" reflects the importance of the declaration.

Group-level framework

Effective processes underpinning the declaration are built on a foundation of a clearly defined methodology and a framework that supports board reporting going forward. This incorporates a well-defined group-level approach to risk assessment, with consistent criteria applied across all areas, ensuring accuracy and eliminating ambiguity. While many organisations adapt currently used tools and processes, we are also seeing the development of separate processes and the implementation of new tools to seamlessly link declaration statements to the underlying data to enable monitoring and ad-hoc reporting to satisfy board requirements.

Focus on what matters

Establishing a clearly defined materiality threshold should ensure that the risk assessment process remains focused and effective, leading to the identification of the right number of controls for the organisation – those that directly address the most material risks. This approach allows for streamlined control activities, fosters productive discussions with the board regarding risk coverage and should support the approach on assurance.

Right level of assurance

Organisations are leveraging the scoping exercise to review, assess and adapt their current level of assurance to incorporate assurance over material controls. What distinguishes successful organisations is their consideration of assurance within the context of business-as-usual (BAU) activities and overall business value. These organisations also recognise that third-party support in the short or medium term may be an optimal solution where internal resources are limited or deployed elsewhere.

A culture of continuous improvement

Successful organisations view Provision 29 not as a one-time hurdle but as an opportunity to realise the broader benefits of a robust risk management framework, such as improved decision-making, enhanced stakeholder confidence and a stronger overall control environment. They foster a culture of continuous improvement by building into the process the regular evaluation of the controls framework, operating culture and the skillset required. This proactive approach should ensure that the resulting BAU process remains relevant and effective in the face of evolving risks and regulatory landscapes.

Suggested structure for the Code Provision 29 disclosure

The Code Provision sets out three elements to be disclosed:

1. A description of how the board has monitored and reviewed the effectiveness of the framework

GUIDANCE

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. (para 294)

The board should describe the main features of the framework, including an overview of the relevant governance structures in place, how the company assesses risks, how it manages or mitigates them, and how information is shared throughout the organisation and how different units interact and communicate. (para 293)

SUGGESTED: an explanation which provides a clear line of sight from the company's purpose, strategy and business model, to the principal risks, decisions around risk appetite (which then dictates the level of controls put in place to keep risks within the agreed risk appetite) through to the assurance and oversight activities which support the board in making the declaration on the effectiveness of the material controls.

2. A declaration of effectiveness of the material controls as at the balance sheet date

GUIDANCE

While the board decides which controls are material these could include, but are not limited to, controls over:

- risks that could threaten the company's business model, future performance, solvency or liquidity and reputation (i.e. principal risks).
- external reporting that is price sensitive or that could lead investors to make investment decisions, whether in the company or otherwise.
- fraud, including override of controls.
- information and technology risks including cybersecurity, data protection and new technologies (e.g. artificial intelligence). (para 272)

SUGGESTED: wording for the declaration:

> **"On the basis of the review, monitoring and assurance activities described on pages X and X, the board confirms that the material controls (as defined on page X) were operating effectively as at the balance sheet date...[any exceptions—see below]."**

SUGGESTED: an explanation of how material controls have been determined including what considerations of materiality have been used (e.g. thinking about the interests of key stakeholders).

SUGGESTED: an explanation of what assurance has been obtained over the effective design, implementation and operation of the materials controls and that the determination of a control being "effective" does not mean that a risk is eliminated, it is that the control is keeping the identified risk within an agreed risk appetite or tolerance.

3. 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

SUGGESTED: further wording for the declaration in relation to material controls which have not operated effectively:

> **"...with the following exceptions: [list the details of any material controls not operating effectively as at the balance sheet date and what action taken or proposed][also consider any control issues through the year that may have been fixed by the year end but which were in the public domain and so should be referenced]. We also provide an update on the actions in relation to matters previously reported [suggest that this should include any material controls issue reported in the previous annual report (even if not under the 2024 Code)]"**

Appendix

What is difference between the Code approach and the US approach under Sarbanes-Oxley?

	UK	US
Source of requirement	Requirements set out in a principles-based code with no associated mechanism for penalty or sanction	Requirements set out in legislation with associated sanctions
Reference	Code Provision 29 of the UK Corporate Governance Code	Section 404 of the Sarbanes-Oxley Act 2002
Scope	Covers all material controls – including financial, operational, reporting and compliance controls	Covers internal controls over financial reporting
Responsibility	The board has responsibility for establishing and maintaining an effective risk management and internal control framework	Management has responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting
Specific nature of the requirement	Whole board is required to provide a declaration on the effectiveness of material controls in the annual report	The CEO and CFO (management) to provide an attestation on the effectiveness of those internal controls over financial reporting
Evidence required	No specific requirement	Attestation has to be supported by documented evidence for the purposes of the auditors' attestation
Supporting auditors' attestation	No specific requirement for auditor attestation but will fall within the scope of ISA720 where there is specific reference to disclosures made under Code Provision 29	Auditors' attestation required and PCAOB auditing standards issued to support this
Other assurance requirements	Is a matter for the board to determine the nature and extent of assurance obtained	n/a
Disclosure of material weaknesses	No specific requirement—deliberately removed such terminology from the Code Provision	Disclosure of any material weaknesses in controls that would not prevent or detect a material misstatement in the financial statements.
Other disclosure requirement	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.	n/a

Overall alignment

For SEC registrants providing the Section 404 attestation, the testing and assurance work undertaken to support this attestation will be relevant for the financial reporting part of the UK Code declaration on the external reporting controls but further testing and assurance will be required on the other elements of control determined to be included in the organisation's definition of material controls (see page 8). However, there is nothing to suggest that the level of testing and assurance work undertaken to support the US attestation needs to be replicated across the other material control elements—that will be for each board to determine.

Contact us:

Governance team

Claire Faulkner

Tel: +44 20 7007 0116

Mobile: +44 7876 478924

Email: cfaulkner@deloitte.co.uk

Tracy Gordon

Tel: +44 20 7007 3812

Mobile: +44 7930 364431

Email: trgordon@deloitte.co.uk

Corinne Sheriff

Tel: +44 20 7007 8368

Mobile: +447824609772

Email: csheriff@deloitte.co.uk

Integrated risk and control specialists

Sonya Butters

Tel: +44 117 984 1074

Email: sobutters@deloitte.co.uk

Louis Macmillan

Tel: +44 20 7007 3705

Email: lmacmillan@deloitte.co.uk

Sara Tubridy

Tel: +44 20 7007 7651

Email: stubridy@deloitte.co.uk

Andy Morris

Tel: +44 20 7007 3308

Email: admorris@deloitte.co.uk

The Deloitte Academy

The Deloitte Academy provides support and guidance to boards, committees and individual directors, principally of the FTSE 350, through briefings on relevant board topics.

Members receive copies of our regular publications on Corporate Governance and a newsletter highlighting upcoming briefings and recently published insights. A dedicated members' website www.deloitteacademy.co.uk is made available so members can register for briefings and access additional relevant resources.

For further details about the Deloitte Academy, including referring colleagues for membership, please email enquiries@deloitteacademy.co.uk.