



Chartered  
Institute of  
Internal  
Auditors

# UK Corporate Governance Code

Provision 29 Key Considerations

# Foreword

Effective corporate governance is paramount to ensuring the sustainability and integrity of organisations and the [2024 UK Corporate Governance Code](#) (the 'Code') sets forth essential requirements that guide companies to establish sound governance practices. These requirements are designed to enhance accountability, foster transparency, and promote ethical behaviour within corporate structures.

Provision 29 of the Code, which is applicable for periods commencing on or after 1 January 2026, specifically focuses on the Board's monitoring of the risk management and internal controls framework. The Code is not significantly different from the 2018 Code with respect to this provision, continuing to emphasise a 'comply' or 'explain' approach, but it does seek to strengthen reporting requirements in relation to 'material controls'.

Internal Audit (IA) can play a pivotal role in helping firms to achieve the objectives of Provision 29. This document explores the requirements of the Provision and aims to provide guidance to help firms review and develop a framework which will enable their Boards to make a declaration in line with the Code. By adhering to these requirements, companies can not only meet regulatory expectations but can also build trust with their stakeholders, including investors, employees, and the wider community. The role that internal audit can play in supporting firms develop their approach is explained together with, for each of the 8 elements, key considerations that internal audit can include in assurance work.

The Chartered IIA is confident that this document will help UK and Ireland internal audit professionals to understand the role they can play in supporting their organisation with Provision 29 in the Code. We encourage you to engage with the insights presented in this document as we collectively work towards fostering a culture of excellence in corporate governance.



# Contents

01



## Overview

- 1 What has changed in the Code and how IA can help
- 2 Summary of the Code's requirements

02



## Framework & Governance

- 1 Scope
- 2 Material Controls
- 3 Board Monitoring
- 4 Board Review

03



## Reporting & Disclosures

- 1 Risk and Control framework
- 2 Monitor & Review
- 3 Declaration (of material control effectiveness)
- 4 Exceptions

# What has changed in the Code and how IA can help

The principal change in the 2024 UK Corporate Governance code ('the Code') relates to enhanced risk management and internal control requirements detailed within Provision 29, which is effective for accounting periods beginning on or after 1 January 2026.

The new guidance is deliberately not prescriptive with an emphasis on a 'comply or explain' approach, while seeking to enhance Directors' accountability.

## Key changes in the Provision 29

Provision 29 focuses on the company's risk management and internal control framework. While provision in the 2018 code was broad, the new code introduces changes designed to upgrade annual reporting and increase the transparency of disclosures.

### 2018 Code

- Boards to monitor the company's risk management and internal control framework and at least annually **carry out a review** of its effectiveness
- Reference to material controls
- Reporting on the Board's review in the annual report

- Annual report to cover an **explanation of how** the Board has monitored and reviewed the effectiveness of the risk management and internal control framework
- Annual report to include a **declaration on the effectiveness of the material controls** as at the balance sheet date
- Annual report to include a **description** of any **material controls** that have **not operated effectively** and the action to improve them

### 2024 Code

## Role of IA ...

For the Board to declare effectively on the monitoring and review of risk management and internal controls framework, it needs to decide the level of confidence that it may place on the work performed by the first and second line.

IA can play a key role in defining what effectiveness would mean and the target level of confidence that the Board may adopt for the purposes of annual reporting.

Organisations may need to re-align current review activities (internal and external) to help the Board make the declaration. IA can bring insights on the overall assurance activities and provide inputs to the design of the overall framework.

## How IA can help the Board ...

### Target level of confidence

IA can help the Board to determine what target level of confidence would enable the Board to make an effective declaration. This may include placing reliance on internal and external reviews.

### Level of documentation

IA can help the Board to determine what would constitute an adequate level of documentation and evidence to enable the Board declaration in the annual report.

### Review and Monitoring mechanism

IA can provide insights into what can be considered as part of the Board level review and Board level monitoring and what can be the frequency of these reviews.

# Summary of the Code's requirements

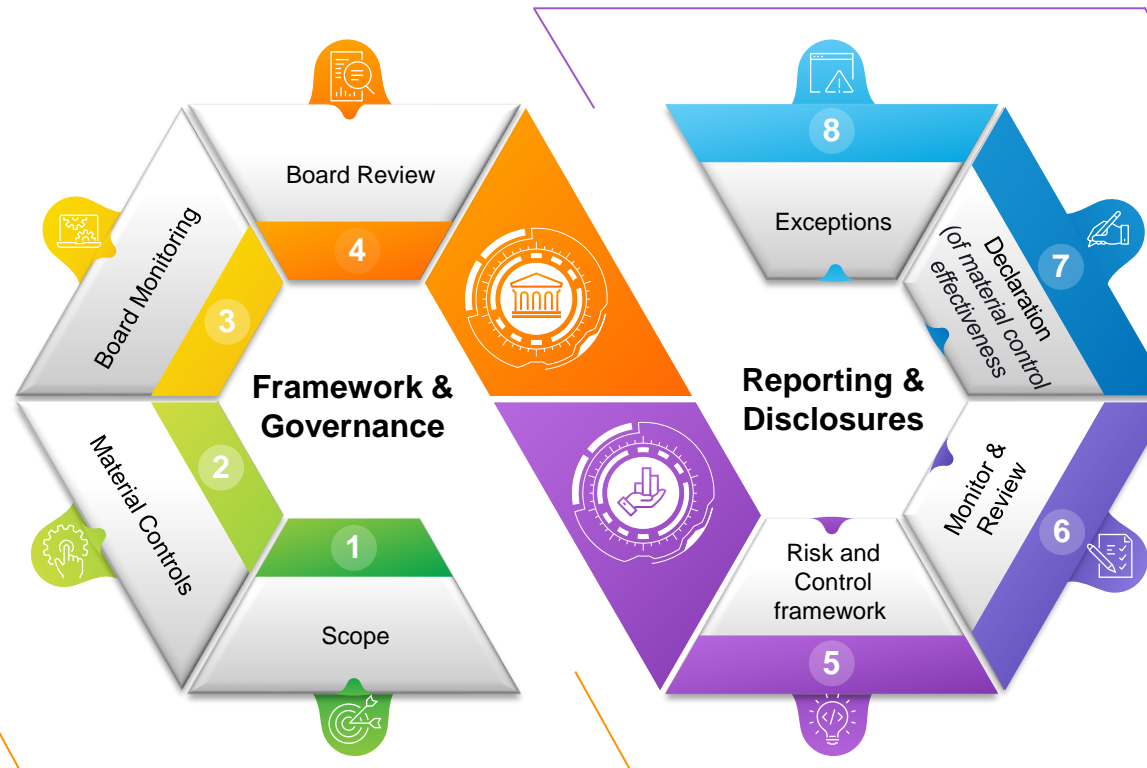
The purpose of this document is to set out the key considerations that Internal Audit functions may reference to help them assess compliance with the Code's requirements. The framework below outlines the building blocks that can be used to facilitate this assessment.

The Code applies to a broad spectrum of organisations and is designed to be flexed according to circumstances. It encourages the application of a proportionate and customisable approach depending on the risk and maturity profile of the organisation applying it.

*FRC Code: Provision 29 extract:*

"The board should **monitor** the company's risk management and internal control framework and, at least annually, carry out a **review** of its effectiveness.

The monitoring and review should cover all **material controls**, including financial, operational, reporting and compliance controls."



*FRC Code: Provision 29 extract:*

"The board should provide in the annual report:

- A description of how the board has **monitored and reviewed** the effectiveness of the **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**."



### Requirements

- The monitoring and review should cover all material controls, including financial, operational, reporting and compliance controls (*FRC 2024 Code: extract Provision 29*).

### Requirements

- Material controls will be company specific and will be different for every company depending on their features and circumstances, including for example size, business model, strategy, operations, structure and complexity. (*FRC Guidance, extract 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. (*FRC Guidance, para. 271*).



### Key considerations

- How has the population of principal risks and material controls been determined and what sources of information have been used to derive population?
- Has consideration been given to principal risks, and where appropriate other risks (such as disclosure risks), as a basis for determining material controls?
- Has the organisation included all relevant types of control in its assessment (i.e. not just financial controls)?
- What stakeholders have been engaged to provide input to the determination of relevant controls (e.g. compliance, finance, technology, internal audit, etc)?
- Has the organisation clearly categorised the different types of controls (e.g. financial, regulatory, fraud, technology) to help demonstrate coverage?

### Key considerations

- Has the Board clearly defined the criteria they have used to identify material controls?
- Has the organisation adopted a pragmatic approach to identifying material controls that address risks specific to their business and align with the defined risk appetite statement?
- Are the material controls proportionate to the principal risks and is there a clear mapping of material controls to the risks they mitigate?
- Are the criteria for determining material controls dynamic and periodically refreshed to capture any new controls and ensure sustainability?
- Has the organisation leveraged already existing risk and internal control focused processes that identify significant controls and provide assurance?
- Has the organisation considered both entity level and transaction level controls to provide an optimal blend of overarching and lower-level controls?
- Has the organisation considered technology related controls as part of its assessment?
- Are the material controls covering both financial and non-financial risk?
- Has the organisation created a central record of material controls?

**Requirements**

- The Board has responsibility for (...) monitoring and reviewing the risk management and internal control frameworks, and the management's process for this, and satisfying itself that they are functioning effectively, and that corrective action is being taken where necessary. *(FRC Guidance, extract para. 215).*
- 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. *(FRC Guidance, extract para. 263).*

**Requirements**

- The board should review the effectiveness of the risk management and internal control framework at least annually (...) or more frequently depending on the circumstances of the company. *(FRC Guidance, extract para. 277).*
- It should ensure that it has considered all material aspects of the framework. *(FRC Guidance, extract para. 278).*
- The review should consider the risk management and internal control framework of the company as a whole. *(FRC Guidance, extract para. 279).*



## Key considerations

- Does the Board receive a sufficient range of information, including both KPIs and metrics as well as qualitative reports, to facilitate their monitoring, throughout the year?
- Does the Board receive regular training on risk management and internal controls to enable them to effectively discharge their oversight responsibilities?
- Is it clear how the information received relates to the material controls identified and does it provide complete coverage across the controls?
- Is the monitoring focused on outcomes and activities rather than processes?
- Is there clear consideration of the company level procedures undertaken to monitor the risk and control framework?
- Are suitable thresholds in place to manage the identification and investigation of exceptions, relative to the defined risk appetite statement?
- Are exceptions subject to a formal review and assessment process with clear conclusions drawn, actions taken and follow-ups to conclusion/remediation?
- Is the frequency of monitoring considered to be proportionate to the organisation's size and complexity?
- Is there appropriate reliance placed on any relevant work performed by the three lines of defence?
- Is the Board monitoring formally evidenced with the records retained?

## Key considerations

- Has the organisation conducted a review which is separate from the ongoing monitoring undertaken but includes an assessment of that monitoring process?
- Is it clear what the Board's target level of confidence is for the determining the effectiveness of material controls and the mechanism by which it will derive that confidence?
- Are the sources of confidence (e.g. self-attestation, third-party assurance) and the level of confidence that each of those sources provides clearly mapped to the material controls?
- Does the review encompass principal risks and material controls from across the whole organisation?
- Is it clear what criteria or basis has been used to undertake the review and do these appear appropriate?
- Does the Board receive a sufficient range of information, including both KPIs and metrics as well as qualitative reports, to facilitate their review?
- Has the Board sourced and considered information from functions or processes that are designed to assess the risk and control framework and whose role is to identify and report control weaknesses (e.g. Controls Office, Operations Risk)?
- Does the Board reach a clear conclusion as to the effectiveness of the material controls and/or does it identify areas for remediation or improvement?
- Is any delegation of responsibility by the Board identified and considered in their overall conclusion?
- Has the review been undertaken sufficiently frequently during the period given the maturity of the risk and control environment and given the extent of change?





## Requirements

- 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. (*FRC Guidance, para. 293*).

## Requirements

- 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. (*FRC Guidance, para. 294*).



## Key considerations

- Does the description include both the risk management and internal control aspects of the framework and is it understandable to an independent reader?
- Is there a description of the end-to-end risk management process from risk identification, to prioritisation and assessment, to ongoing management and review?
- Are the principal risks identified and are the mitigating measures clearly relatable to those risks?
- Does the description provide additional information on risk appetite and horizon risks that may help readers to better contextualise the framework?
- Is there a provision to consider the emerging risks, as and when they arise?
- Is there a description of the governance and committee structure that is employed by the organisation to manage and oversee risks?
- Does the description explain the role of the first, second and third lines of defence in the risk and controls framework? Are there clearly defined responsibilities for each of these lines of defence?
- Does the description provide information in relation to the control profile (e.g. the types and levels of control) and how material controls fit into that profile?

- Does the summary provide an insightful explanation about how the monitoring and review process has operated, as opposed to a high-level confirmation that a review has taken place?
- Does the summary adequately explain the basis upon which the declaration is being made, including sources of information considered, and the governance and committees being leveraged?
- With reference to the information received by the Board, does the summary provide details as to the relevance and impact of this information and any subsequent actions taken in response to the information?
- Is there a mechanism adopted by the Board to perform the monitoring? Has accountability and delegation been clearly documented?
- Does the summary provide details as to the cadence of the monitoring and review process undertaken and is this appropriate for the organisation's size and complexity?
- Is there a level of confidence determined by the Board to report on the effectiveness of framework?
- Does monitoring and review consider both, historic events as well as potential future events, before making the declaration?

## Key considerations



**Requirements**

- The annual report should include a declaration on the effectiveness of the material controls at the balance sheet date. (*FRC Guidance, extract para. 296*).

**Requirements**

- If a material control is not operating effectively at the date of the balance sheet, the board should disclose this in the annual report together with any action taken, or proposed, to improve controls.
- The annual report should also provide a summary of how the board has addressed previously reported issues.  
(*FRC Guidance, extracts para. 297*).



## Key considerations

- Is the declaration succinct, clear and included in an appropriate location (e.g. within the overall governance statement)?
- Is the declaration appropriately focused on the effectiveness of the material controls as opposed to the broader risk and control framework?
- Does the declaration make it clear that it relates to the year-end?
- Does the declaration describe the impact of any disclosable, material events and the associated actions taken, or planned to be taken, to address identified control deficiencies?
- If the effectiveness of controls has not been determined, has the Board provided reasonable explanations to explain why this has not been possible and how this can be potentially addressed in the future?
- Are any relevant post balance-sheet procedures relating to the internal control framework clearly identified and explained as part of the declaration?
- Are the actions taken in relation to previously reported issues included in the declaration?
- Is there an underlying mechanism, with clear accountability, to ensure that correct and complete information is provided in the declaration?

- Is the description of the exceptions sufficiently clear to allow an independent reader to understand the reason for the exception and the associated risk?
- Are the actions proposed to address the exceptions described in sufficient detail and it is clear how they address the associated risks?
- Is the mechanism to monitor the proposed actions clearly articulated and is it commensurate with the severity of the exceptions identified and the level of effort required to remediate them?
- Is the responsibility for monitoring and resolving the exceptions clearly articulated (e.g. through the assignment of specific functions)?
- Do the proposed actions have an appropriate target date for closure?

## Key considerations



Chartered  
Institute of  
Internal  
Auditors

We would like to thank the following individuals for their significant contribution to this paper.



**Andrew Adeoye**

Internal Audit and Controls  
Banking Partner, EY



**David Sooby**

Internal Audit and Controls  
Insurance Partner, EY



**Saheet Gohil**

Internal Audit and Controls  
Banking Partner, EY



**Peter George**

Internal Controls  
Director, EY



**David Khalil**

Internal Controls  
Director, EY



**Deepika Bhargava**

Internal Controls  
Manager, EY



**Sophia Adetutu**

Internal Controls  
Manager, EY



**Ben Parsons**

Internal Controls  
Manager, EY

© 2025 Chartered Institute of Internal Auditors  
© 2024 Ernst & Young LLP