

Preparing for Provision 29 – Risk management and internal controls

Revised UK Corporate Governance Code

In January 2024, the Financial Reporting Council published the revised UK Corporate Governance Code (the “Code”). Provision 29 of the revised Code introduces an enhanced requirement for boards to monitor and review the effectiveness of material controls covering financial, operational, reporting and compliance areas, and to include an explicit declaration of their effectiveness at the balance sheet date.

The enhanced declaration requirement will apply to the Group for the financial year ending 31 March 2027.

Although a formal declaration is not required in respect of the current financial year, the Board and the Audit & Risk Committee (“ARC”) have commenced a structured programme of work to ensure that the Group is fully prepared to meet the new requirements.

Governance and oversight

The Board has overall responsibility for the Group’s system of risk management and internal control and for reviewing its effectiveness. The ARC supports the Board in discharging these responsibilities through regular review of:

- The group’s principal and emerging risks
- The design and operation of key controls
- The effectiveness of the three lines of defence governance model
- The development of the Group’s approach to Provision 29

During the year, the ARC has reviewed management’s assessment of the scope of material controls and the proposed roadmap to support compliance with Provision 29. Preparation for the enhanced declaration is now embedded within the ARC’s forward agenda and forms part of the Committee’s ongoing oversight of risk and internal controls.

Three lines of defence

The Group operates a three lines of defence model in governance.

- First line: management ownership of risks and controls within business units and central functions
- Second line: oversight and challenge from Risk, Compliance and Finance functions, including aggregation and reporting through the Enterprise Risk Management (“ERM”) framework
- Third line: independent assurance provided by Internal Audit and, where appropriate, external assurance providers

This framework underpins the Board’s assessment of principal risks and the associated mitigations, as described in the Risk management section of this report.

Identification and mapping of material controls

Provision 29 requires boards to focus specifically on “material controls”. The Group has adopted a structured and proportionate approach to identifying such controls, taking into account:

- Controls mitigating principal risks
- Controls supporting financial and regulatory reporting
- Operational and resilience controls, including technology and data governance
- Compliance controls relating to the group’s regulatory obligations

Using the Group’s ERM platform, management is mapping key controls to principal risks and risk appetite statements. This process enables clearer articulation of control ownership, documentation of control design and enhanced monitoring of operating effectiveness.

Particular focus areas during the year have included:

- Financial reporting and accounting controls
- Technology and data governance, including cybersecurity and operational resilience
- Third-party and outsourcing risk management
- Fraud risk management and economic crime controls
- Business continuity and disaster recovery arrangements, including defined recovery time and recovery point objectives

This work provides the foundation for the future Board declaration and supports enhanced transparency in external reporting.

Preparing for Provision 29 – Risk management and internal controls

Strengthening assurance and internal audit

The Board has previously resolved to enhance the Group's internal assurance capability in line with peer practice and evolving governance expectations. During the year, further progress has been made in developing a risk-based internal audit programme aligned to the Group's principal risks.

The Internal Audit plan is informed by inherent risk and control assessments and focuses on areas of higher residual risk, including:

- IT general controls and information security
- Risk management processes and governance
- Finance and reporting controls
- Regulatory compliance

Internal Audit activity is conducted in accordance with applicable professional standards and is reported to the ARC at each meeting. Where relevant, the Group continues to obtain third-party assurance, including ISAE 3402 reporting, to supplement the internal assurance framework.

In parallel, management attestation processes are being formalised to support future Board reporting on the effectiveness of material controls.

Roadmap to FY27 declaration

The Board's roadmap to full compliance by 31 March 2027 includes:

- Finalisation of the material controls universe and documentation of control design
- Completion of initial operating effectiveness testing across priority control areas
- Further development of the Internal Audit plan to provide appropriate third-line coverage
- Enhancement of management attestations and evidence retention
- Continued ARC oversight and Board engagement
- Pilot drafting of the proposed Directors' declaration during FY26

The Board is satisfied that the programme of work is proportionate to the Group's size, complexity and risk profile and is progressing in line with the implementation timetable set out in the revised Code.

Conclusion

The Board is committed to maintaining a robust system of risk management and internal control that supports the Group's long-term strategy and protects the interests of Shareholders and other Stakeholders.

Provision 29 represents an important evolution in Board accountability and transparency. The Group has taken proactive steps to strengthen its governance framework, enhance assurance and clarify the identification and monitoring of material controls. Further updates will be provided in future reporting periods as the Group moves towards full compliance with the revised Code.