Provision 29: Implications for GRC and Compliance Professionals

Provision 29 of the 2024 UK Corporate Governance Code introduces a fundamental reform in how organisations assess, evidence, and publicly report the effectiveness of their risk management and internal control systems.

Effective from 1 January 2026, it transforms assurance into a board-level responsibility that demands credible evidence, integrated oversight, and a culture of transparency.
For GRC professionals this is both a compliance challenge and a strategic opportunity to embed assurance at the centre of governance.

Reframing Corporate Assurance for a New Era of Board Accountability

How GRC leaders can turn the 2026 UK Corporate Governance reform into a strategic opportunity for integrated, evidence-led assurance.

1. The Governance Reset
Why Provision 29 marks a turning point in board-level accountability.

2. The New Standard of Assurance
From monitoring to declaring control effectiveness with evidence.

3. Mapping the Risk Universe
Identifying what truly matters in risk and control effectiveness.

4. From Data to Confidence
Building integrated, evidence-based assurance ecosystems.

5. UK Corporate Governance Code Provision 29 Readiness
Turning regulation into a structured implementation roadmap.

6. Culture, Conduct, and the Future of Assurance
Embedding ethics, behaviour, and intelligence-led monitoring into governance.

1. The Governance Reset

The Financial Reporting Council (FRC) introduced Provision 29 following a series of high-profile governance failures that revealed major gaps in board visibility over key control weaknesses.

Objectives of Provision 29

- Rebuild stakeholder and investor confidence.
- Strengthen board accountability for internal control effectiveness.
- Drive integration between risk, audit, and compliance functions.
- Move corporate culture from tick-box compliance to continuous assurance.

Scope: All companies applying the UK Corporate Governance Code.
Effective date: Accounting periods beginning on or after 1 January 2026.

2. What Provision 29 Requires

Provision 29 introduces an explicit duty for boards to monitor, review, declare, and disclose.

Board duties include:

1. Continuous monitoring of the risk and control framework.
2. Annual review of control effectiveness.
3. Formal declaration of control effectiveness in the annual report.
4. Disclosure of material weaknesses and remediation plans.

These declarations must be evidence-based, not assumed. Boards should use multiple assurance sources - management self-assessments, compliance testing, and internal/external audits to substantiate their claims.

Strategic takeaway: this moves UK governance towards a model closer to U.S. SOX, where evidence-based assurance becomes the currency of board credibility.

3. Mapping the Risk Universe

Defining material controls that truly matter.

The Code does not define “material controls,” but boards and GRC teams must decide which controls are critical to principal risk management.

Material controls typically exhibit these traits:

- Linked to principal risks or business-critical processes.
- Failure would cause financial, reputational, or regulatory damage.
- Supported by ownership, documentation, and operational testing.

Guiding frameworks:

- COSO Internal Control – Integrated Framework (2013)
- ISO 31000 Risk Management (2018)
- FRC Guidance on Risk Management and Internal Control (2024)

Practical action: Develop a Material Controls Register linking each principal risk to its owner, assurance source, and evidence location.

4. From Data to Confidence

Building an integrated, evidence-based assurance ecosystem.

Provision 29 encourages a connected-risk model, where assurance is not siloed between audit, risk, and compliance but integrated into a single ecosystem.

Best practices include:

- Centralised control registers and consistent risk taxonomies.
- Unified dashboards linking key risk indicators (KRIs) and key performance indicators (KPIs).
- Automated exception tracking and real-time visibility for board committees.
- Assurance mapping to demonstrate control coverage and accountability.

The outcome: Evidence-backed decision-making and transparent reporting.

5. Risk Domains and Control Examples

Provision 29 extends across all domains that materially influence an organisation's strategic resilience.

Risk Domain	Examples of Material Controls	Primary Assurance Sources
• Financial Reporting & Accounting	Reconciliations, fraud controls, treasury oversight	Finance, Internal Audit
• Operational & Business Continuity	Supply-chain resilience, disaster recovery, change management	Risk Management, Operations
• Compliance & Legal	AML/CTF, GDPR, sanctions, anti-bribery	Compliance, Legal
• Strategic & Business Model	M&A governance, scenario testing, investment reviews	Board, Risk Committee
• People & Conduct	Whistleblowing, misconduct handling, remuneration alignment	HR, Ethics
• ESG & Sustainability	Emissions reporting, supplier audits, human rights due diligence	ESG, Third-Party Assurance
• Technology & Cyber	Access management, encryption, incident response plans	IT Security, External Audit

Boards should prioritise controls most critical to long-term stability and align them with clear ownership and testing cycles.

6. Evidence and Assurance

Provision 29 mandates credible, auditable evidence for each material control.

Assurance should assess:

- Design effectiveness: adequacy of control design
- Operating effectiveness: consistency of execution
- Monitoring effectiveness: escalation and remediation tracking

Assurance sources:

1. First line – management self-assessments
2. Second line – risk and compliance testing
3. Third line – internal audit or external assurance

Building a Controls Assurance Map that connects each control to its owner, assurance source, and evidence repository enhances both traceability and accountability.

7. Culture, Behaviour and Leadership

Provision 29 explicitly links culture to control effectiveness. Boards must ensure:

- Ethical tone from the top
- Training on control ownership
- Safe communication on errors or near misses
- Cultural assessments via surveys and audits

A healthy control environment depends on cultural maturity and behavioural alignment.

8. Provision 29 Implementation Roadmap for GRC Teams

GRC leaders should adopt a phased roadmap to achieve Provision 29 compliance and maturity.

Phase 1: Diagnostic Review

Assess current risk and control frameworks against FRC standards to identify assurance gaps and priorities.
Deliverable: Gap Analysis Report.

Phase 2: Define Material Controls

Map principal risks to key controls, assign ownership, set testing criteria, and document materiality rationale.
Deliverable: Material Controls Register.

Phase 3: Enhance Assurance

Strengthen first, second, and third line testing aligned to control criticality for credible, proportionate assurance.
Deliverable: Integrated Assurance Plan.

Phase 4: Integrate Data and Reporting

Consolidate assurance data into shared dashboards, unify risk libraries, and automate oversight reporting.
Deliverable: Unified Assurance View.

Phase 5: Board Engagement and Training

Train directors on Provision 29 duties and conduct a dry-run declaration supported by verifiable evidence.
Deliverable: Draft Board Declaration.

Phase 6: Continuous Improvement

Embed ongoing monitoring, remediation, and cultural reviews to sustain long-term assurance maturity.
Deliverable: Sustainable Assurance Framework.

9. Common Challenges and Lessons Learned

Common difficulties in implementing Provision 29 include:

- Unclear materiality criteria
- Fragmented assurance functions
- Poor documentation and evidence management
- Over-reliance on internal audit
- Limited cultural oversight

Success factors:

- Defined governance ownership
- Integrated assurance framework
- Transparent and continuous reporting
- Strong culture of accountability and learning

Conclusion: From Obligation to Opportunity

Provision 29 challenges Operational, Compliance, and Procurement leaders to prove—not just claim—control effectiveness. The real struggle lies in fragmented assurance data, rising regulatory scrutiny, and limited time to produce credible evidence.

This is the moment to move from reactive compliance to proactive assurance.

Strategic actions for OCP leaders:

- Centralise control and assurance data for unified visibility
- Embed continuous monitoring to detect risks early
- Integrate intelligence-led evidence into board reporting
- Train leaders to interpret assurance insights with confidence

With Neotas, assurance becomes more than a statement it becomes proof of resilience, integrity, and trust.

How Neotas Can Help

Neotas strengthens control frameworks and assurance readiness through intelligence-led, data-driven insights.

Third-Party and Supply Chain Integrity

Continuously monitor third parties through OSINT and adverse media to detect sanctions, reputational and integrity risks early.

Conduct and Culture Risk

Analyse behavioural and digital footprints to reveal misconduct patterns and provide actionable culture insights for HR and ethics teams.

Cyber and Data Exposure

Map external threat surfaces, detect data leaks, and generate verifiable evidence to validate IT security control effectiveness.

ESG and Ethical Compliance

Verify supplier sustainability and human-rights claims while continuously monitoring ESG risks across non-financial control areas.

Integration with Assurance Frameworks

Feed validated intelligence into GRC dashboards, providing independent evidence that strengthens board declarations and assurance transparency.

LET'S CONNECT www.neotas.com/contact-us

Stay tuned with the latest industry insights on our **LinkedIn** page.

APPENDIX A

Material Controls Mapping Template

Principal Risk	Material Control	Control Owner	Assurance Source	Evidence Type / Location	Frequency
Financial misstatement	Monthly reconciliations	CFO	Internal Audit	GL reports	Monthly
Data breach	Access management controls	CIO	IT Security	Access logs	Quarterly
Regulatory non-compliance	AML monitoring programme	Head of Compliance	Compliance	Training records / monitoring logs	Quarterly
Operational disruption	Business continuity testing	COO	Risk Committee	DR test reports	Annual

Note:

Use this template to link each principal risk to its control, owner, and evidence source. Updating it quarterly ensures traceability, accountability, and readiness for Provision 29 board declarations. Integrating Neotas intelligence data further validates external assurance evidence, strengthening overall control effectiveness and governance transparency.

APPENDIX B

Provision 29 Readiness Checklist

Use this checklist to benchmark your organisation's progress toward full compliance and assurance maturity under Provision 29.

Checklist

1. Governance & Oversight

- □ Board and Committees briefed and trained on Provision 29 expectations
- □ Roles and responsibilities for assurance clearly defined and approved
- □ Risk, Audit, and Compliance Committees aligned on reporting approach
- □ Material controls formally reviewed and endorsed by the board

2. Risk & Control Framework

- □ Principal risks identified, assessed, and mapped to control owners
- □ Materiality criteria for controls defined and documented
- □ Control objectives, testing methods, and review frequency established
- □ Risk-control linkages validated through independent review

3. Assurance & Evidence

- □ Assurance sources mapped across first, second, and third lines
- □ Evidence repositories centralised and access-controlled
- □ Assurance testing results documented, reviewed, and tracked
- □ Independent validation completed for high-risk control areas

4. Reporting & Disclosure

- □ Assurance dashboards aligned with FRC guidance and metrics
- □ Draft narrative disclosure prepared for annual report inclusion
- □ Board declaration rehearsed through a dry-run review
- □ Material weaknesses and remediation plans transparently recorded

5. Continuous Improvement

- □ Monitoring cycles established to review assurance effectiveness
- □ Findings from audits and reviews systematically remediated
- □ Cultural and behavioural indicators integrated into assurance metrics
- □ Lessons learned documented and shared with governance stakeholders