EXECUTABLE GRC

Provision 29 Compliance Checklist.

The five areas of documented readiness a board needs to stand behind a credible declaration on the effectiveness of its material internal controls.

- Governance framework
- Risk & materiality
- Control design
- Testing & monitoring
- Board declaration

Aligned to **Provision 29 of the UK Corporate Governance Code (2024)** and the FRC's internal controls guidance. Each item requires documented, contemporaneous evidence — not assertion.

Gabriel Few-Wiegratz · SureCloud

Published 29 June 2026

HOW TO USE THIS CHECKLIST

Work the five areas as a readiness assessment.

Each item requires documented, contemporaneous evidence, not assertion. Work through all five areas, then use the gaps to build your programme.

What Provision 29 requires, and when

APPLIES FROM

Financial years beginning on or after 1 Jan 2026.

Takes effect for these reporting periods.

FIRST DECLARATIONS

Annual Reports published in 2027.

The first declarations reach shareholders here — **evidence must be in hand before year end.**

IN SCOPE

UK premium-listed companies on the LSE.

Others may adopt the approach as good practice.

The five areas of documented readiness

1	Governance framework	Accountability, oversight and a Board-approved assessment methodology.
2	Risk & materiality	Material risks mapped to controls, with a documented materiality threshold.
3	Control design	Each material control described, owned and held in a system of record.
4	Testing & monitoring	Risk-based, independent testing with deficiencies rated and remediated.
5	Board declaration	Consolidated output reviewed, position determined, disclosure retained.

START THE FRAMEWORK AND MATERIALITY WORK NOW

The two areas that gate everything downstream — governance and materiality — take longest to stand up. Begin them immediately: leaving testing to the final quarter leaves no room to remediate before the declaration date.

1

AREA ONE

Governance framework.

Provision 29 makes internal-controls effectiveness a Board responsibility. Before any control is tested, the accountability, oversight and methodology have to be in place — and documented — so the eventual declaration rests on an approved process rather than an ad-hoc exercise.

- [ ] The Board has formally designated accountability for overseeing the internal controls assessment — the Audit Committee in most cases.
- [ ] Audit Committee terms of reference have been updated to include Provision 29 oversight responsibilities.
- [ ] A named executive holds responsibility for the internal controls framework — CFO, CRO, or CISO for the relevant control categories.
- [ ] A cross-functional controls working group is established, with representation from Finance, Risk, Legal, IT/Cyber and Compliance.
- [ ] A documented methodology for the Provision 29 assessment has been approved by the Audit Committee. **BOARD-APPROVED**
- [ ] The FRC guidance on Provision 29 has been reviewed and the company's approach aligned to it.
- [ ] The assessment methodology and timeline have been communicated to all control owners.

ACCOUNTABILITY IS THE FOUNDATION, NOT A FORMALITY

A declaration is only as credible as the process behind it. Designating clear accountability and an approved methodology early means every downstream test, exception and remediation slots into a governance structure the Board already owns — rather than being reconstructed under pressure at year end.

2 Risk and materiality assessment

Identify the material risks, map controls to them, and define what level of control failure would be reportable under Provision 29.

- [ ] A complete list of material risks facing the company has been identified and documented, drawing on the enterprise risk register.
- [ ] For each material risk, the relevant controls have been identified and mapped.
- [ ] A materiality threshold has been defined and documented: what level of control failure would be reportable under Provision 29? THRESHOLD
- [ ] The materiality determination has been reviewed and approved by the Audit Committee.
- [ ] Controls tied to FCA and PRA regulatory obligations and FCA PS21/3 operational resilience requirements have been included where applicable.
- [ ] Third-party and ICT outsourcing controls have been assessed for materiality — particularly for DORA in-scope entities or firms with material outsourcing under SS2/21.

3 Control design and documentation

Every material control described, assessed for adequacy, owned, and held in a system of record that supports version history and evidence linkage.

- [ ] Each material control has a documented description: what it does, who is responsible, how often it operates, and what evidence it produces.
- [ ] Control designs have been assessed for adequacy — if operating as designed, is the control sufficient to address the risk?
- [ ] Control owners have confirmed their understanding of, and responsibility for, each control.
- [ ] The controls inventory is held in a system of record that supports version history and evidence linkage. GRC PLATFORM, NOT SPREADSHEET
- [ ] Gaps in the control universe — risks identified without adequate controls — have been documented and escalated.
- [ ] Compensating controls for known design weaknesses have been identified and documented.

4

AREA FOUR

Control testing and monitoring.

A risk-based testing programme, run independently of control owners, produces the evidence the declaration rests on. Deficiencies must be rated, tracked and closed — with ongoing monitoring filling the gaps between formal testing cycles.

- [ ] A risk-based testing programme has been designed and approved, covering all material controls.
- [ ] Testing frequency reflects control risk: higher-risk controls tested more frequently, automated controls tested for continued operation.
- [ ] Testing has been carried out by teams independent of control owners — internal audit or second-line risk functions. **INDEPENDENCE**
- [ ] Test results have been documented with evidence, including any exceptions or deficiencies identified.
- [ ] Deficiencies have been rated by severity: control deficiency, significant deficiency, or material weakness equivalent.
- [ ] Remediation actions for deficiencies have been assigned, tracked and closed within defined timelines.
- [ ] An ongoing monitoring process is in place between formal testing cycles — KRIs, automated control monitoring, exception reporting.
- [ ] Evidence from regulatory inspections, external audits and internal audit reviews has been incorporated into the controls assessment.

5

AREA FIVE

Board declaration and reporting.

The final area turns the assessment into a Board position. The Audit Committee reviews the consolidated output, the declaration position is determined and documented, and the disclosure — with any exceptions — is reviewed by Legal before it reaches the Annual Report.

- [ ] The Audit Committee has reviewed the consolidated output of the controls assessment, including all deficiencies and their disposition.
- [ ] The Board has received a summary with sufficient detail to support an informed declaration.
- [ ] The declaration position — effective, effective with exceptions, or not effective — has been determined and documented.
- [ ] Where exceptions are identified, the nature of the weakness, its impact, and the remedial actions taken are documented for the Annual Report.
- [ ] The Provision 29 disclosure in the Annual Report has been reviewed by Legal and the Audit Committee before publication.
- [ ] The controls assessment documentation is retained and accessible for a minimum of six years. 6-YEAR RETENTION

THE DECLARATION POSITION, IN THREE WORDS

Effective means material controls operated as intended across the period. **Effective with exceptions** discloses identified weaknesses alongside the remediation under way. **Not effective** is reserved for material weaknesses that undermine the controls as a whole. Whichever applies, the position must be evidenced — not asserted.

POWERED BY GRACIE

BUILD YOUR PROVISION 29 EVIDENCE FRAMEWORK

The declaration challenge is evidence, not controls.

Gracie AI Agents — with Personas and Skills — reduce manual evidence collection by up to 65%, giving your Audit Committee real-time visibility across Provision 29, FCA operational resilience, DORA and ISO 27001 in one integrated GRC programme.

Up to 65%	5 areas	1 programme
Less time spent on manual evidence collection	Assessed for gaps before the declaration date	Provision 29, DORA, FCA resilience and ISO 27001

FULL GUIDE	**FCA Provision 29 Compliance Checklist**	surecloud.com/resource-hub
FRAMEWORK	**UK Corporate Governance Code 2024**	surecloud.com/resource-hub
RELATED	**Operational Resilience & DORA Readiness**	surecloud.com/resource-hub
PLATFORM	**Continuous Control Monitoring with Gracie**	surecloud.com/resource-hub

Book a personalised demo.

See how Gracie AI Agents and Skills automate the evidence collection, monitoring and audit-trail work Provision 29 demands — across your whole GRC programme.

Book a demo →