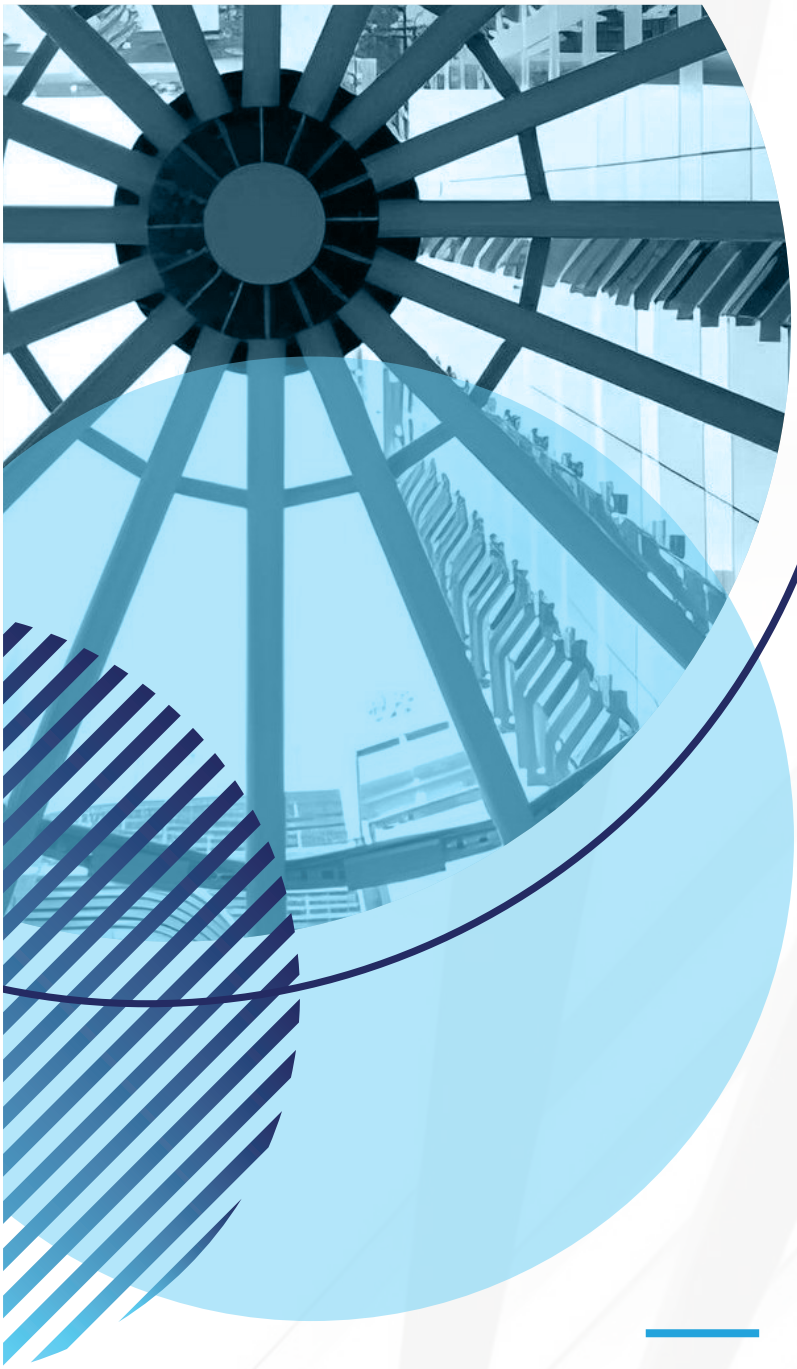


Enterprise Resilience vs *Crisis Management*

Solving the Board-Level Accountability Problem

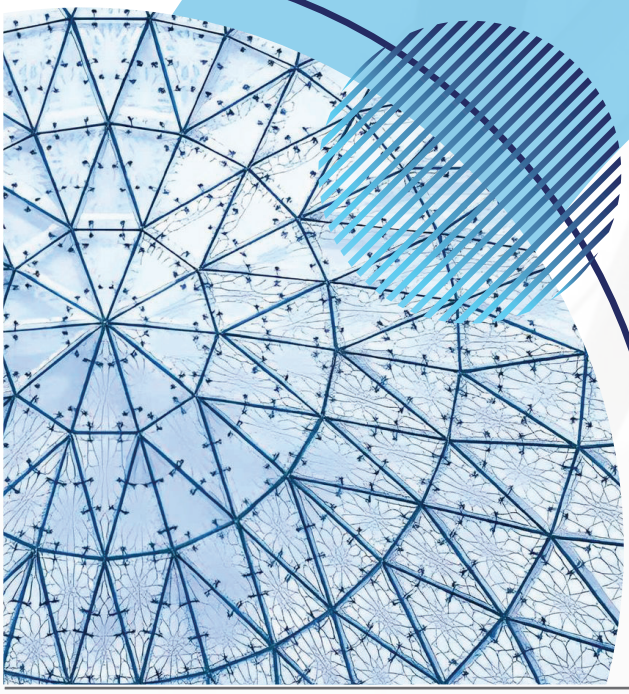
Most UK boards believe they are prepared for disruption. Fewer can demonstrate it. That gap — between perceived readiness and genuine resilience governance — is the defining boardroom challenge of 2026.

Insights

The terms enterprise resilience and crisis management are used interchangeably by too many UK leadership teams. They are not the same thing. One is a proactive, board-mandated strategic capability built into how an organisation operates every single day. The other is an operational response triggered after something has already gone wrong. Treating them as synonymous leaves organisations exposed, regulators unsatisfied, and boards personally vulnerable in an environment where governance accountability has never been more stringent.

The Core Distinction

ENTERPRISE RESILIENCE AND CRISIS MANAGEMENT ARE NOT THE SAME THING



The distinction matters because it determines where board accountability begins and ends. Under the 2026 UK Corporate Governance Code, that question is now a matter of mandatory, outcomes-based reporting — not optional best practice. Boards must demonstrate that their governance structures actually work, not simply that they exist on paper.

DIMENSION	ENTERPRISE RESILIENCE	CRISIS MANAGEMENT
Nature	Proactive, strategic capability	Reactive, incident response
Horizon	Long-term — embedded in strategy	Immediate — post-disruption
Board role	Governance, oversight, investment	Oversight during incident
Ownership	Explicit board-level mandate required	Often delegated to IT/ops
Measure of success	Threats absorbed, minimal disruption	Speed of recovery
Risk of failure	Strategic drift, competitive erosion	Operational & reputational

Crisis management without enterprise resilience is fire-fighting. Enterprise resilience without crisis management is a strategy that has never been tested under real conditions. UK boards in 2026 need both — but must be explicit about which one they are governing and which they are delegating.

The Accountability Problem

WHERE UK BOARDS ARE FALLING SHORT

The accountability gap is real, structural, and present across UK organisations of every size. It is not driven by bad intentions — it is driven by a set of deeply embedded governance habits that the current risk environment is rendering increasingly dangerous.

Confidence Without Capability

Many UK directors feel broadly confident in their board's overall effectiveness, yet that confidence does not extend to specific resilience and compliance capabilities. The gap between perceived governance readiness and actual governance capacity is where the greatest risk lives.

Blind Spots Without Action

A significant proportion of UK boards recognise that they have governance blind spots — particularly around cybersecurity, AI risk, and third-party dependencies — but have not structurally addressed them. Recognition and action are not the same thing.

Technology Risk Is Not Governed

Most UK boards still treat technology resilience as an IT function rather than a board-level governance responsibility. Yet critical digital service failure translates directly into customer access loss, revenue disruption, and market confidence erosion — with consequences that land squarely in the boardroom.

Plans Without Evidence

Many boards have resilience plans in place but cannot produce evidence that those plans are operating effectively. Under the 2026 UK Corporate Governance Code's formal internal controls statement requirement, documented policy alone is no longer sufficient.

REGULATORY POSITION — 2026

The 2026 UK Corporate Governance Code mandates evidence-backed internal controls reporting across financial and non-financial risks, rejecting boilerplate disclosures.

Meanwhile, the Economic Crime and Corporate Transparency Act introduces a “failure to prevent fraud” offence and expands director accountability—making enterprise resilience a clear board-level legal duty

Key Insights

WHEN A MAJOR OPERATIONAL DISRUPTION OCCURS

> *"The board that believes it is ready for a crisis, but has never tested that belief against documented evidence, is not resilient. It is overconfident — and overconfidence is a risk in itself."*

When a major operational disruption occurs — whether driven by a cyber incident, a technology platform failure, a third-party collapse, or a regulatory investigation — the question that boards and regulators ask is not whether a plan existed. It is whether the board understood it, owned it, and had ensured it was genuinely fit for purpose.

Root Causes

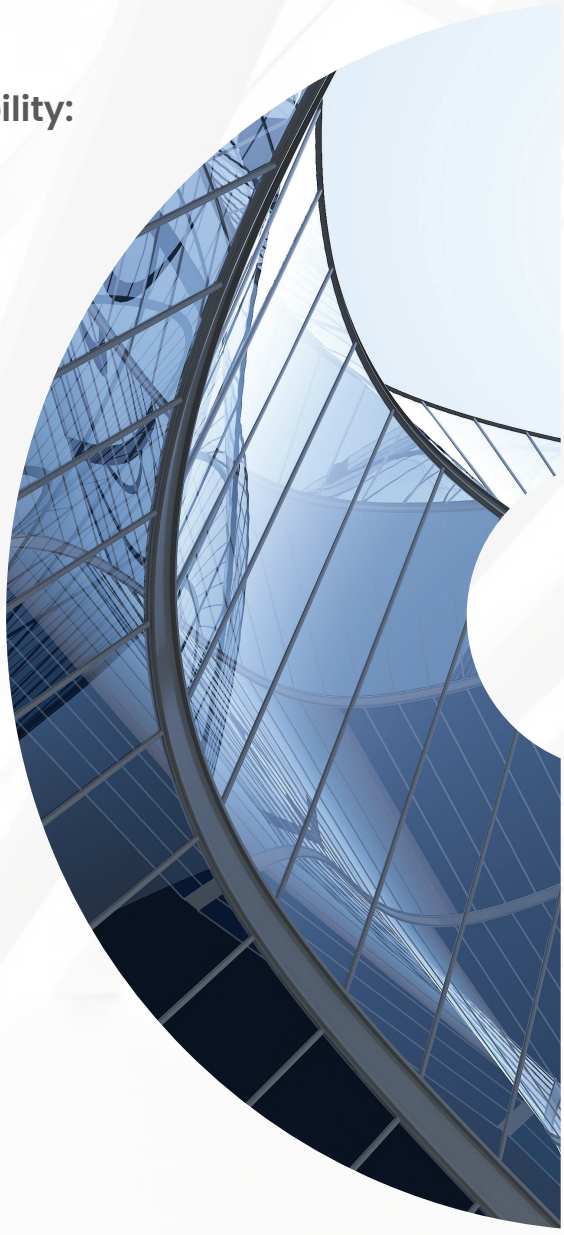
WHY UK BOARDS KEEP FAILING ON RESILIENCE GOVERNANCE

The board-level accountability gap does not generally arise from negligence. It follows four structural problems that most UK boards have yet to fully resolve — and that the 2026 governance environment is making it increasingly costly to leave in place.

01

Resilience Is Built For Compliance, Not Capability:

Organisations that treat resilience as a regulatory exercise—rather than a real capability—tend to underperform during disruption. A plan built for compliance is not the same as one built for a crisis. Boards relying on the former may carry greater governance risk than they anticipate.



02

Ai And Technology Risk Sit Outside Board Governance:

Cybersecurity and AI are key risk areas where many UK boards still lack structured oversight. Often treated as technical issues, their impact ultimately affects financial performance, compliance, and reputation at the board level. The 2026 governance framework now expects clear, documented oversight—not just awareness.

03

The Board-management Boundary Is Undefined In Practice:

Most UK boards understand their crisis role, but few clearly define and test the line between governance and execution. This gap creates decision bottlenecks during crises, costing time, credibility, and value.

04

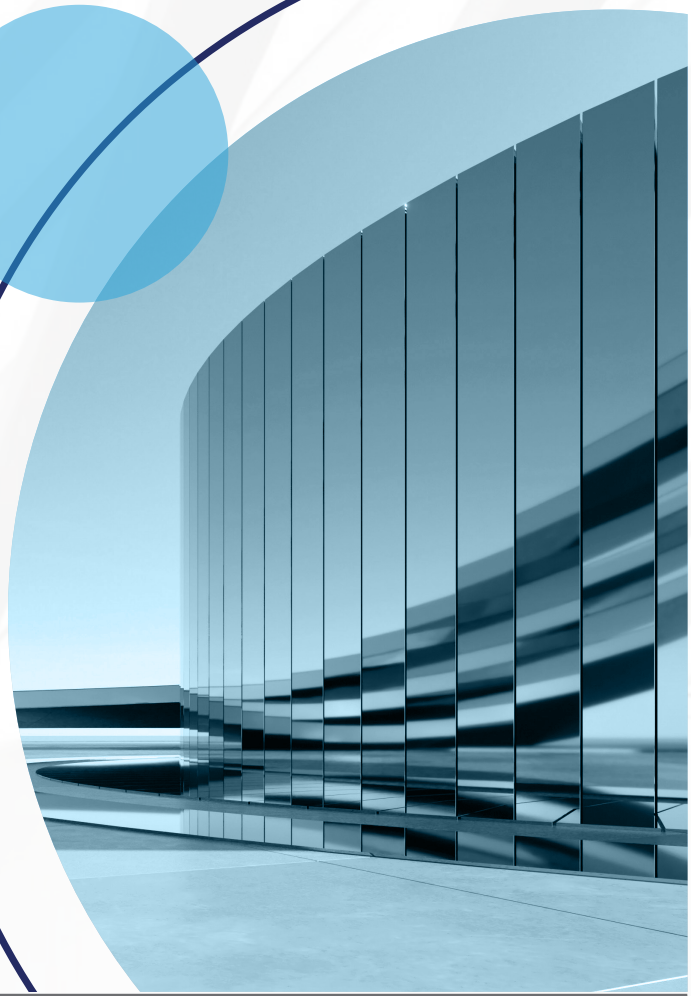
Resilience Investment Is Disconnected From Strategy:

UK regulators expect resilience to be embedded in strategy, not treated as a separate function. When seen as a cost centre, it fails in practice—because resilience disconnected from business direction cannot protect it.

The Solution

CLOSING THE ACCOUNTABILITY GAP: FIVE GOVERNANCE IMPERATIVES

Enterprise resilience governance is not a single intervention. It requires sustained board attention across five interconnected areas — each of which maps directly to Insights UK's Management Consultancy service areas.



01 Strategy Integration

Resilience must be embedded into the organisation's strategy — not appended to it. Board decisions on market focus, investment, and operating model must explicitly account for resilience trade-offs as a core input, not an afterthought.

02 Governance & Accountability Design

Clear, documented delineation of board versus management responsibilities across a full range of disruption scenarios — not just in principle, but in board-approved frameworks that have been tested and can be evidenced.

03 Structural Resilience

Operating models that are over-reliant on single vendors, markets, or digital platforms cannot be made resilient by planning alone. Structural change is often required — and the 2026 Code's outcomes-based framework makes that need visible.

04 Operational Stress-testing

Resilience plans must be tested against multiple realistic scenarios — cyber, AI failure, third-party collapse, geopolitical disruption, regulatory investigation — not just the most recent or most familiar type of incident.

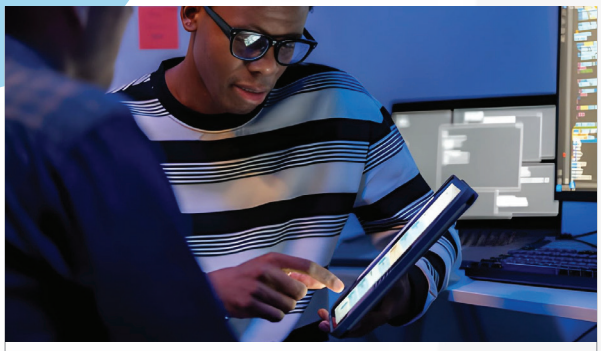
05 Internal Audit & Controls

Independent verification that resilience governance is actually operating as intended — not just documented. Under the 2026 Code's Provision 29, boards must formally attest to the effectiveness of internal controls across both financial and non-financial risks.

How Insights UK Can Help You

FOUR STAGES OF RESILIENCE GOVERNANCE JOURNEY

If your board is facing any of the challenges mentioned, Insights UK can provide the structured, senior-level support needed to move from exposure to confidence. We work with UK boards and leadership teams across four stages of the resilience governance journey.



STAGE -1

Diagnosis

We help boards understand where the accountability gap actually sits — not where it is assumed to sit.

- Independent review of existing resilience and crisis management frameworks against the 2026 UK Corporate Governance Code requirements.
- Assessment of where the board-management boundary is unclear, untested, or undocumented.
- Identification of structural fragilities in the operating model that planning alone cannot address.
- Gap analysis across strategy, operations, risk, and internal controls.

STAGE -2

Framework Design

We build governance frameworks that work under real pressure — not just on paper.

- Design of board-level accountability structures with clear ownership across disruption scenarios.
- Development of resilience frameworks aligned to the 2026 Code's formal internal controls attestation requirements
- Integration of resilience trade-offs into strategic planning and investment decision processes.
- Governance design for risk at the board level, with documented escalation pathways.

STAGE -3

Testing & Stress-testing

We test resilience plans against the scenarios that matter most — not just the most familiar ones.

- Multi-scenario stress-testing covering cyber, third-party collapse, geopolitical disruption, and regulatory investigation.
- Cross-functional crisis simulation exercises with board involvement.
- Post-exercise review and documented framework improvements.
- Ongoing calibration as the threat and regulatory landscape evolves.

STAGE -4

Implementation & Assurance

We stay engaged through delivery — not just diagnosis.

- Programme governance and change management support throughout the implementation of resilience improvements.
- Internal audit and controls review to provide boards with independent assurance that frameworks are operating as intended.
- Restructuring support where operating model changes are required to address structural fragility.
- Ongoing advisory to boards as regulatory requirements develop under the 2026 Code and the Economic Crime and Corporate Transparency Act.

Contact Us

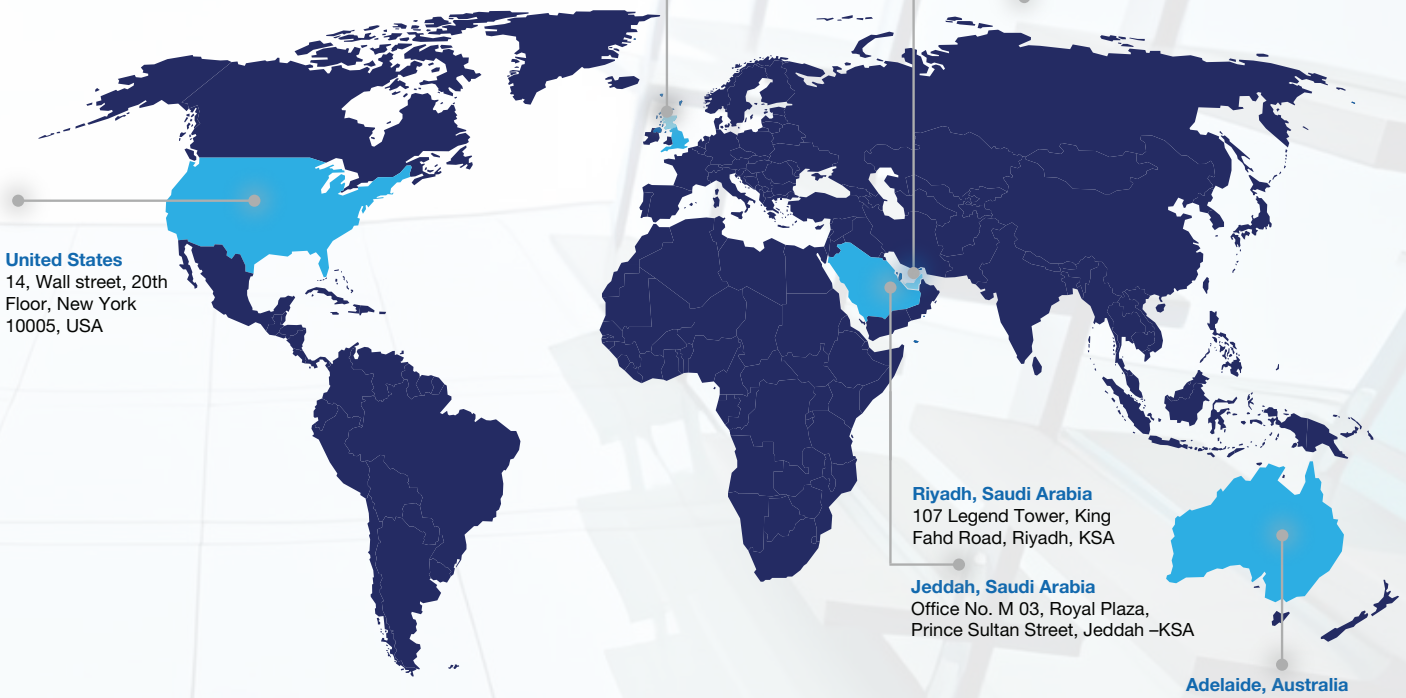
For further information, clarification and discussion concerning the contents, please contact:

Amir Jhangeer
Country Head - United Kingdom
: ajhangeer@insightss.co

London, United Kingdom
37th Floor, 1 Canada Square, London E14 5AA

Leeds, United Kingdom
7 Park Row 1st Floor Leeds LS1 5HD United Kingdoma

United Arab Emirates
Office 711, Iris Bay Building, Business Bay, Dubai – UAE



United States
14, Wall street, 20th Floor, New York 10005, USA

Riyadh, Saudi Arabia
107 Legend Tower, King Fahd Road, Riyadh, KSA

Jeddah, Saudi Arabia
Office No. M 03, Royal Plaza, Prince Sultan Street, Jeddah –KSA

Adelaide, Australia
P.O. Box 6387, Halifax Street, Adelaide 5000, Australia

Insights
Navigating Complexity, Simplifying Success