QUOD ORBIS

Operational Resilience at the Board Table

A Strategic Playbook for 2026 and Beyond

How Boards Can Govern Resilience, Cyber, AI, and Business Continuity in a Disruptive World

Contents

Executive summary

What This Playbook Delivers

- Clear, practical governance for business resilience
- Boards equipped to challenge cyber, AI and operational risk with confidence
- A unified view of cyber, AI, third-party and operational dependencies
- Stronger board–CISO alignment and decision-making
- A shift from reactive response → continuous assurance

What Boards Must Understand

✓ Operational resilience is business resilience
✓ Cyber is now the primary threat to business continuity
✓ AI is accelerating risk faster than organisational maturity
✓ Regulations (DORA, NIS2, AI Act) expect continuous, real-time assurance
✓ Annual, point-in-time reporting is no longer sufficient

What's Shifting in How Boards Oversee Cyber

✓ Technical metrics → business impact
✓ Point-in-time audits → continuous visibility
✓ Siloed risk → end-to-end resilience
✓ "Compliance" → protecting the ability to operate

Why the CISO Relationship Now Matters More Than Ever

Boards can't govern resilience alone. This playbook helps you:
✓ Translate cyber activity into board-level outcomes (revenue, continuity, visibility)
✓ Elevate the CISO from technical lead to strategic business partner
✓ Make security investments based on impact, not tools
✓ Give security teams the board-level backing they need to reduce exposure

Why This Matters Now

✓ Cyber risk is no longer a technical issue – it is a business resilience issue.
✓ Digital disruption now directly affects revenue, operations, customers and reputation.
✓ Boards must govern the organisation's ability to operate, not just its security posture.
✓ This playbook gives directors the clarity and structure needed to do that confidently.

Chapter 1: Why Resilience Now Sits at the Board Table

From Cyber Oversight to Business Accountability

Operational resilience is no longer a technical function it is a board-level responsibility. Boards must ensure the organisation can operate, serve customers, protect revenue, maintain trust, and survive disruption, whether caused by cyberattacks, AI failures, supply chain breakdowns, or operational incidents.

Board takeaway

Cyber, AI, and technology risks are business risks. Boards must own them like financial and strategic risks. Strategic oversight, proactive governance, and continuous monitoring turn resilience from a compliance obligation into a competitive advantage.

Key points

- **End-to-end regulatory expectation:** Regulators now expect boards to govern resilience across all critical functions, including technology, operations, and third-party dependencies.
- **Real-time insight over reports:** Boards need dashboards and KPIs that translate operational, cyber, AI, and supplier risks into clear business impact NOT quarterly summaries.
- **Resilience as a strategic enabler:** Operational resilience should align with organisational objectives, supporting growth, innovation, and competitive advantage, always underpinning that with the need to drive customer trust.
- **Reputation and stakeholder trust:** Failures in resilience can damage brand, customer confidence, investor trust, and employee engagement.
- **Cross-functional accountability:** Boards must ensure clear ownership across IT, operations, HR, legal, and supply chain, with escalation paths for crisis response.
- **Scenario planning and stress testing:** Boards should oversee exercises that model potential disruptions and assess readiness of critical services and the effectiveness of incident response playbooks.
- **Culture of risk awareness:** Operational resilience requires a proactive, risk-aware organisational culture that anticipates threats and mitigates impact. Board needs to be leading this drive within the organisation.
- **Third-party and supplier risk:** Boards should monitor concentration, resilience, and dependency mapping to understand exposure beyond internal operations.

\\ Chapter 2: Operational Resilience What Boards Are Accountable For

Boards are accountable for setting expectations, approving tolerances and investment, and assuring themselves that management has built and tested resilience capable of protecting customers, the market and the organisation during severe disruption.

Board Accountability

Identified and prioritised critical business services
→ The board is accountable for ensuring this has been done credibly and aligns to strategy and risk appetite.

Defined impact tolerances and recovery expectations
→ Approval and challenge sit with the board (customer harm, financial loss, regulatory thresholds).

Established clear ownership and decision rights
→ Governance and accountability structures are a board responsibility.

Maintained effective governance and escalation structures
→ Boards are accountable for ensuring escalation works under stress, not just on paper.

Invested appropriately in resilience capabilities
→ Investment decisions and trade-offs against risk exposure are a core board duty.

Maintained transparent communication readiness
→ Boards are accountable for confidence that the organisation can communicate clearly with regulators, customers, and markets in a crisis.

How Boards Exercise Oversight and Assurance

Boards provide oversight by challenging management's assumptions, testing the credibility of preparedness, and seeking assurance that resilience capabilities remain effective as the business, technology and threat landscape evolve.

Board Oversight & Assurance

Assessed operational dependencies
→ Board ensures coverage is end-to-end and includes material third-party and concentration risks.

Tested resilience through scenarios and stress events
→ Board challenges scenario severity, realism, and whether results change decisions.

Implemented meaningful resilience metrics
→ Board ensures metrics are decision-useful and outcome-focused, not technical vanity metrics.

Ensured lessons learned are acted upon
→ Board holds management to account for sustained improvement, not box-ticking.

Strategic Lens

- Which products/services are mission-critical?
- What risks threaten continuity or trust?
- Are recovery and governance sufficient?
- Are third-party dependencies resilient and protected?
- Do dashboards show full operational resilience?
- Are escalation and communication clear in crises?
- Are lessons driving resilience improvement?

Why This Matters for Boards

Operational resilience failures are no longer "IT issues."

They are board-level events with consequences for:

- Customer harm
- Regulatory intervention
- Financial loss
- Reputation and shareholder confidence

Boards are judged not by whether incidents occur, but by whether they exercised effective oversight beforehand.

Board takeaway

Operational resilience is a strategic responsibility. Boards must ensure that critical services, internal teams, and third-party partners can withstand disruption. By actively monitoring dependencies, measuring performance, and enforcing accountability, boards protect customers, revenue, and reputation while turning resilience into a competitive advantage.

\\ Chapter 3: Cyber Risk as the #1 Threat to Operational Resilience

Why Boards Must Treat Cyber as a Strategic Business Risk

Cyber risk is no longer a technical issue delegated to IT or security teams:

- It is the single most common trigger of operational disruption.
- It can halt critical services.
- It can damage customer trust.
- It can erode shareholder value.

For boards, cyber risk must be governed as a core component of operational resilience, not as a standalone security function.

How Cyber Disruption Translates Into Business Impact

From a board perspective, cyber risk should always be viewed through a business impact lens:

- Disruption or unavailability of critical services
- Revenue interruption or loss
- Customer harm, loss of trust, or regulatory breaches
- Delay or derailment of strategic objectives

The board's question is no longer "Are our systems secure?" but "Can the organisation continue operating if a cyber attack occurs?"

Why Cyber Sits at the Centre of Operational Resilience

Most operational failures today are digital, including ransomware, outages, data corruption, and third-party breaches, causing:

- Prolonged service disruption
- Regulatory scrutiny and enforcement
- Financial loss and recovery costs
- Reputational damage and customer churn

Cyber incidents do not stay contained within systems, they cascade across people, processes, suppliers, and customers.

Key Amplifiers of Cyber Risk

Several factors amplify cyber risks, creating vulnerabilities that can disrupt even well-prepared organisations:

- Third-party exposure – Supplier and cloud risk
- Complex IT – Hybrid, legacy, fast-changing
- Evolving threats – Ransomware and attacks
- Ripple effects – Incidents cascade broadly

Cyber risk rarely appears as a single-point failure. It emerges through interconnected dependencies the organisation may not see.

Board-Level Metrics That Matter

Boards should focus on outcome-driven indicators, not technical activity:

Area	Metric	Business Lens
Critical Service Disruption	Hours of downtime	Customer harm, revenue & impact
Incident Response	Time to detect, respond & recover	Resilience effectiveness
Third Party Exposure	% of critical suppliers assessed	Dependancy risk
Data Breach Impact	Financial & reputational lost	Trust & valuation
Recovery Readiness	Backup & recovery test success	Ability to resume operations

These metrics help boards understand residual risk, not just effort expended.

Strategic Lens

- Which cyber risks could realistically stop our most critical services?
- How confident are we in our ability to recover under real-world conditions?
- Where do third-party dependencies increase our exposure?
- Does our cyber risk appetite align with our tolerance for disruption?
- Are we seeing leading indicators of increased operational fragility?

Board takeaway

Cyber risk is a strategic business risk, not a technical one. Boards that embed cyber oversight within operational resilience governance are better positioned to protect critical services, safeguard trust, and support sustainable growth.

\\ Chapter 4: The AI Wild West — Strategic Oversight and Guardrails for Boards

Why AI Changes the Risk Equation

Artificial intelligence is rapidly reshaping how organisations operate, offering significant benefits while introducing new risks:

- Increased efficiency, automation, and innovation
- New operational, cyber, and reputational risks
- Governance models not designed for these emerging challenges

For boards, AI represents a fundamental shift in the risk landscape.

Why AI Feels Like the "Wild West"

AI risk feels uniquely unpredictable because:

- Adoption outpaces governance, with employees using AI without formal oversight
- Speed and scale amplify the impact of errors
- Threat actors weaponise AI through automated phishing, deepfakes, social engineering, and malware
- Controls lag behind adoption, with no consistent global standards for AI oversight, auditing, or accountability

The result is high-impact risk with limited visibility.

The Regulatory Landscape (Still Catching Up)

Global regulation is evolving, but unevenly:

- EU: The Artificial Intelligence Act (in force from August 2024) introduces binding, risk-based obligations with phased implementation
- UK: A principle-based, adaptive approach prioritising innovation with accountability
- US: Fragmented, agency-led and state-driven guidance with no overarching federal framework

Boards cannot rely on regulation alone to manage AI risk. Governance must lead compliance, not follow it.

Real-World Implications for Operational Resilience

AI introduces new failure modes that boards must understand:

- Disruption at scale from automated attacks or system dependencies
- Reputational damage from deepfakes, misinformation, or biased outcomes
- Regulatory exposure from unlawful or opaque AI use
- Service continuity risks when AI-driven processes fail or behave unpredictably
- Amplified cyber risk from AI-enabled threats

Boards must treat AI risk as a strategic priority, not just a technical issue.

Strategic Lens

- Which AI systems directly affect critical services or customer outcomes?
- What happens if an AI-driven process fails or behaves unexpectedly?
- How are AI risks monitored and escalated at board level?
- How do third-party AI dependencies affect recovery and continuity?

Board-Level Guardrails for AI Oversight

Boards should focus on strategic guardrails, not technical controls:

Guardrail	Board Oversight Focus
Accountability	Named executives responsible for AI outcomes and risk
Transparency	High-risk AI systems documented and reported
Performance & Safety	Metrics tied to critical services and business outcomes
Data Governance	Input/output data protected, auditable and compliant
Ethics & Bias	Oversight of fairness and reputational exposure
Third-Party AI	Vendors assessed against resilience objectives
Regulatory Alignment	Compliance with AI Act and sector requirements

These guardrails ensure AI remains an enabler of resilience, not a source of instability.

Board takeaway

AI is a powerful accelerator — of both opportunity and risk. Boards that govern AI proactively, with clear accountability and visibility, can protect operations, reputation and trust while enabling safe innovation.

\\ Chapter 5: The Boardroom Playbook for Digital Operational Resilience

From Insight to Action: Dashboards, Metrics, and Accountability

Introduction

This chapter gives boards a practical playbook for governing operational resilience. You'll learn how to:

- See the organisation's resilience and cyber posture at a glance
- Align with CISOs and security teams to translate technical efforts into business outcomes
- Use dashboards, KPIs, and KRIs to make informed, strategic decisions
- Ensure the board can protect operations, revenue, reputation, and customer trust

\\ 5.1 Digital Operational Resilience Summary

Boards need a clear, strategic view of resilience, but must also understand and align with cyber security teams to ensure operational continuity.

Key elements of a resilience dashboard:

- Status of critical services, dependencies, and impact tolerances
- Overall resilience posture with trend indicators
- Key emerging risks; AI, ransomware, third-party
- Regulatory compliance overview

Board takeaway

Boards should expect summary dashboards that give a high-level view, highlighting areas requiring attention without diving into technical minutiae.

\\ 5.2 KPI/KRI Summary (Strategic)

Boards are accountable for key performance and risk indicators to ensure resilience. KPIs (Key Performance Indicators) and KRIs (Key Risk Indicators) should focus on business-critical outcomes, not just technical completion metrics.

- KPIs show how well the organisation is performing against operational goals and service expectations.
- KRIs highlight potential threats to these outcomes, giving boards a forward-looking view of risk exposure.
- Combining these metrics enables boards to make informed, strategic decisions about investments, risk appetite, and operational priorities.

Example areas to review

Focus Area	Metric	Target	Current	Trend	Board Action
Service Continuity	% Critical Services Operational	99.9%	99.7%	↓	Review contingency plans
Cyber & Data Risk	Potential Business Impact Score	Low	Moderate	↑	Escalate mitigation strategy
AI & Automation	High-risk AI Systems Reviewed	100%	60%	↑	Approve oversight measures
Third-Party Risk	Critical Supplier Coverage	100%	90%	↔	Review top suppliers
Incident Preparedness	Recovery Readiness	100%	95%	↔	Confirm crisis playbooks

Board takeaway

KPIs and KRIs should link directly to critical services, revenue exposure, and operational continuity. They are a tool for strategic decision-making, not just reporting.

5.3 Frameworks and Governance

Boards need a clear view of which frameworks, standards, and regulations govern the organisation and how well these are being applied. This isn't about understanding technical details — it's about strategic oversight and decision-making.

Key points for boards:

Coverage

Which frameworks and regulations are relevant?

Examples:

- ISO 22301 (Business Continuity)
- DORA (Digital Operational Resilience)
- NIS2 (Network & Information Systems Security)
- AI governance policies and controls

Status

Are these frameworks fully implemented, partially applied, or still in progress?

- Dashboards should provide a traffic-light view (green = compliant, amber = in progress, red = gaps).

Gaps & Board Decisions

Highlight where board attention or approval is required, such as:

- Investing in controls to meet regulatory obligations
- Authorising additional resources to close compliance gaps
- Prioritising remediation of critical vulnerabilities

Example in practice:

"Our DORA implementation covers 80% of critical services, but key third-party dependencies are not fully mapped. Board decision needed: approve additional third-party oversight and monitoring."

Board takeaway

This section ensures boards see the compliance landscape at a glance, know where their intervention is needed, and can link compliance gaps directly to business risk and operational impact.

5.4 Organisation and Accountability

Boards are ultimately accountable.
Beyond that, boards also need to understand who is accountable at team level for resilience, cyber, and operational continuity, and how decisions flow across the organisation. In fact, Boards need to ensure they lead the clarity in this area and support and ensure faster decision-making, clear ownership, and effective incident response.

Key points for boards:

Roles and Committees:

Identify the owners of key functions:

- Risk Committee: oversees enterprise risk and operational resilience
- Critical Service Owners: responsible for continuity of business-critical processes
- Incident Response Leads: manage response to cyber or operational disruptions

Example in practice:

"A ransomware incident triggers the incident response lead, who notifies the CIO and CISO. The CISO escalates operational impact metrics to the board within 24 hours, enabling informed decision-making."

Decision-making and Escalation:

Use RACI diagrams to clarify:

- Responsible: Executes tasks or actions
- Accountable: Final decision-maker
- Consulted: Provides input or expertise
- Informed: Receives updates

Board takeaway

This section ensures lines of accountability are clear, responsibilities are understood, and boards can trust that operational and cyber risks are being managed effectively.

Incident Escalation:

Boards should know when and how they'll be briefed during a crisis. For example:

- Minor incidents: reported in monthly dashboards
- Major disruptions: immediate board notification with recovery plan

\\ 5.5 Bridging the Board: The CISO Gap

Boards don't need to be technical experts, but they can build strategic alignment with the CISO to gain real insight into cyber risk and resilience.

Structured Reporting Rhythm

- In the current climate, boards should require monthly executive reports highlighting business impact, KPIs/KRIs, incidents, near misses, and third-party exposure.
- Focus on business impact, not technical minutiae.

Joint Strategic Planning

- Include the CISO in board-level strategic discussions and scenario planning.
- Ensure cyber and AI risk are integrated into business planning and operational resilience strategies.

Risk Appetite and Investment Alignment

- Define cyber risk appetite in terms of business and operational outcomes.
- Prioritise investments based on business impact, enabling the CISO to allocate resources strategically.

Dashboards and Metrics

- Use dashboards combining all cyber, AI, operational, and third-party risk as well as regulatory compliance.
- Translate technical risk into business-relevant insights for informed board decisions.

Encouraging Communication and Strategic Partnership

- Promote open communication and clear escalation pathways.
- Treat the CISO as a peer-level strategic partner influencing operational, resilience, and regulatory decisions.

\\ 5.6 Translating Cyber Risk into Board Language

Boards should focus on business impact, not technical detail, allowing CISOs to become strategic partners:

Ask the right questions

Service impact, financial/reputational exposure, tolerance for disruption.

KPIs and dashboards

Show cyber risk as business-relevant metrics (service availability, regulatory impact, incident potential).

Strategic decision-making

Include CISOs in operational planning, investments, and regulatory compliance decisions.

Board support

Encourage CISOs to communicate risks in business terms, not technical jargon.

Board takeaway

Speaking business language, defining risk appetite, and integrating dashboards and metrics enables the CISO to act as a strategic partner, turning cyber security into a resilience driver.

5.7 Cyber Speak → Board Speak: A Practical Cheat Sheet

One of the biggest challenges boards face is understanding the CISO's language. Technical updates often highlight activities rather than business impact. To govern effectively, boards need to see how cyber efforts protect revenue, operations, and customer trust.

Let's translate the CISO's language as to what it means for the Board:

CISO:	Board Translation
We blocked 4 million attacks	We prevented $2M in potential revenue disruption
We're patching critical CVEs	We closed risks that could stop business operations
We need security monitoring	Without visibility, we won't know if operations are impacted until it's too late
We added threat intelligence	We are focusing on our most likely weaknesses, using industry data to protect critical operations
We completed pen testing	We validated our defences against real-world attack scenarios
We maintain compliance	We have operational advantages to win regulated markets
We completed a risk assessment	We identified risks that could cause $2M/day losses and have plans to reduce them
We're adding to disaster recovery	We've improved our ability to recover operations from an outage or breach
We completed an IR tabletop	We tested our resilience plans and improved business recovery
We deployed MFA	We reduced the chance of account compromise impacting operations
We need more budget for tools	A $250k investment can protect $1M/day of operational risk
Phishing fail rates are 15%	Most staff are trained not to expose data; we have plans for remaining staff

Board takeaway

This is about aligning the CISO's priorities and relating that to the impact on the overall business.

- This isn't about simplifying technical work it's about aligning cyber security actions to business strategy, resilience, and measurable outcomes.
- Encourage the CISO to frame updates in business terms for board decisions.
- Ensure dashboards and KPIs reflect business-relevant impact, not just technical completion metrics.

Actionable guidance:

- Ask for metrics tied to critical services, operational impact, and financial exposure.
- Request business-oriented summaries for board meetings.

Use these translations as a framework to hold the CISO accountable while understanding the strategic value of cyber security initiatives.

\\ Chapter 6: Looking Ahead: The 12-24 Month Roadmap for Board-Level Resilience

From Oversight to Action: Preparing the Organisation for a Disruptive Future

Operational resilience requires sustained board leadership. The next 12–24 months are critical for embedding continuous oversight, strengthening governance, and building the capability to withstand cyber, AI, supplier, and operational disruption.

Board Questions to Anchor the Roadmap

- "Are dashboards delivering a complete, real-time picture of operational and AI risk within the first quarter?"
- "Which services pose the highest risk today — and what is the plan to address them this year?"
- "Are recovery and mitigation plans strong enough to protect revenue and customer trust?"
- "Are governance structures and accountabilities clear before scenario tests begin?"
- "Are resilience investments delivering measurable outcomes year-on-year?"

0-3 Months: Establish Establish Visibility Across Critical Services

Objective: Create a shared, factual understanding of what really matters.

- Identify key cyber, operational, cloud, AI, and third-party dependencies.
- Highlight single points of failure and concentration risk.
- Define initial impact tolerances for service disruption.

Board focus: What would hurt the business most if it failed tomorrow — and do we actually understand why?

3-6 Months: Integrate Operational, Cyber, and AI Risk

Objective: Build a unified view of risk and dependency.

- Connect cyber, operational, supplier, and AI risks to critical services.
- Invest in continuous monitoring, automation, analytics, and assurance.
- Identify exposure points that threaten service continuity.
- Align risk assessments across teams to remove silos and duplication.
- Prioritise risks based on business impact, not technical severity.

Board focus: Where are we most exposed — and which risks could cascade into a major incident?

6-9 Months: Strengthen Governance and Accountability

Objective: Ensure the right people are empowered.

- Update governance and committee structures to reflect integrated risk.
- Assign clear ownership for cyber, AI, third-party, and operational resilience.
- Define escalation paths and decision thresholds.
- Test crisis roles, handoffs, and communications.

Board focus: If disruption happens at 2 a.m., who is accountable — and who has authority to act?

9-12 Months: Define Metrics That Matter

Objective: Move from reporting activity to measuring resilience.

- Establish KPIs and KRIs for:
  - Service continuity
  - Cyber readiness
  - Supplier concentration and failure risk
  - AI and automation exposure
- Integrate metrics into dashboards with thresholds and alerts.
- Link resilience performance to financial, customer, and regulatory outcomes.

Board focus: Are we measuring what matters to the business — or just what is easy to report?

12-18 Months: Test Resilience Under Realistic Stress

Objective: Build muscle memory for disruption.

- Run scenario planning and tabletop exercises covering:
  - Cyber attacks
  - AI failure or misuse
  - Supplier collapse
  - Major service outages
- Stress-test recovery plans against worst-case scenarios.
- Validate that tolerances, recovery times, and playbooks are realistic.

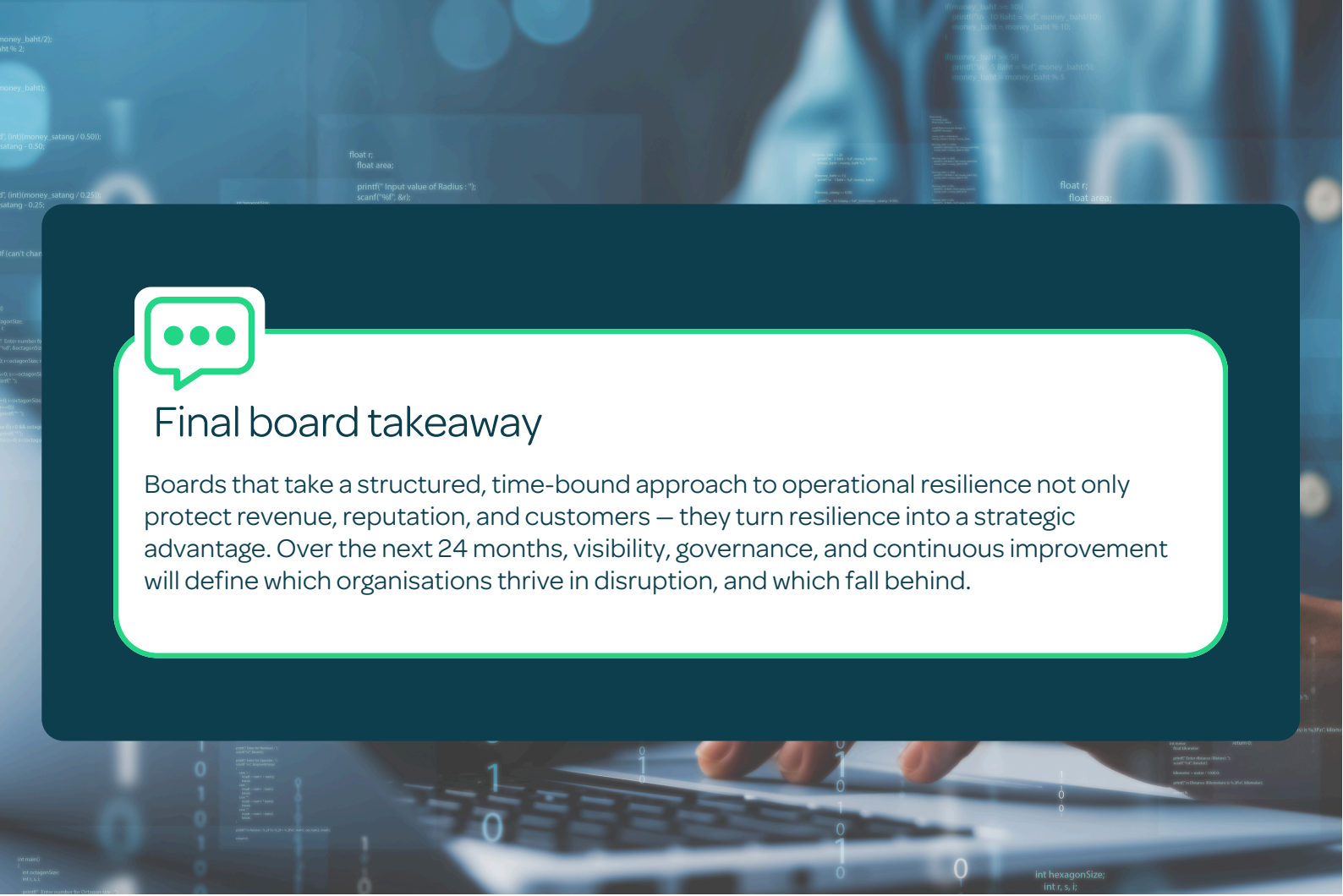
Board focus: Could we withstand a high-impact incident — and how quickly could we recover?

18–24 Months (and ongoing): Continuous Improvement

Objective: Turn resilience into a competitive advantage.

- Review resilience maturity annually and benchmark against peers.
- Embed lessons learned into governance, metrics, and operations.
- Demonstrate year-on-year improvement to regulators, customers, and investors.

Board focus: Is our resilience improving — or quietly falling behind market expectations?



Final board takeaway

Boards that take a structured, time-bound approach to operational resilience not only protect revenue, reputation, and customers — they turn resilience into a strategic advantage. Over the next 24 months, visibility, governance, and continuous improvement will define which organisations thrive in disruption, and which fall behind.

QUOD ORBIS

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2025

Winner
Market Leader in Continuous Controls Monitoring!

Contact Us

www.quodorbis.com

contact@quodorbis.com

+44(0)203 9622206

Quod-Orbis