

Board Cyber Governance & Assurance Reporting Framework



IG-Smart Ltd · Practical Guide Collection · 25 October 2026

General information and original working aids; not legal advice, certification, clinical authorisation or regulatory approval.
NHS identity appearing in retained illustrative artwork does not imply NHS approval or endorsement.

Use this guide to make a better-evidenced decision. This is general information and an original working aid, not a client-specific legal opinion, certification, clinical safety authorisation or regulatory approval. Apply the relevant jurisdiction, current requirements and competent professional review to your circumstances. Examples are illustrative unless expressly attributed.

Your first three steps

1. Choose one consequential business service and the decision leadership needs to make.
2. Separate management assertions, verified evidence and independent assurance.
3. Use the one-page briefing to record the decision, owner and evidence needed next.

From technical findings to accountable executive decisions: a reference model for boards, audit and risk committees, CISOs and virtual CISOs

Executive proposition: A dashboard is not assurance. Boards need to know which consequential digital services are exposed, what evidence supports management's confidence, what is outside tolerance, who owns remediation and which decisions require board authority.

For: board and audit committee chairs, non-executive directors, CEOs, CISOs, CROs, CIOs, General Counsel, internal auditors and regulators' relationship owners. **Purpose:** turn scattered cyber metrics into a decision-oriented reporting discipline. **Boundary:** this is an illustrative IG-Smart governance method, not a regulatory-approved risk score, legal opinion, penetration test or promise of protection.

Executive briefing — the five questions a board report must answer

1. **Consequence:** Which important products, services, operations or populations could be harmed by a cyber event?
2. **Exposure:** Which plausible incidents could cause that harm and where are critical dependencies concentrated?
3. **Evidence:** What independent and management evidence supports the claimed control effectiveness, and how current is it?
4. **Decision:** Which risks exceed approved tolerance, what trade-offs exist and who has legal or delegated authority to accept them?
5. **Accountability:** Who will make the change, by when, how will the outcome be verified and what will bring it back to the board?

A competent board pack should enable a decision in minutes while linking each conclusion to inspectable evidence. The UK's Cyber Governance Code of Practice organises director actions into **risk management, strategy, people, incident planning/response/recovery, and assurance/oversight**. Those are five complementary lines of oversight, not an external certification, legislation or a mandatory uniform report format. The April 2025 Code offers governance guidance; obligations arise separately from applicable law, regulation, contracts and directors' duties. [S1][S2]

1. Why cyber board packs commonly fail

Technical dashboards commonly show counts of patches, phishing clicks, SOC alerts and red/amber/green trends. These may support management oversight, but a shrinking vulnerability count can conceal one unremediated exploitable issue affecting a critical service. Likewise, certification may demonstrate a management system within an identified scope without proving that every supplier, cloud configuration or recent incident is adequately controlled. A risk heatmap can help triage discussion, but cannot alone establish loss probability, patient harm or the sufficiency of assurance.

The report must distinguish **risk, control, assurance, exception, decision** and **action**. The board should receive proportionate, decision-ready material rather than operational telemetry presented without consequence.

A useful report also avoids invented precision. Estimates of financial loss should disclose input assumptions, source, scenario, uncertainty and calculation owner; illustrative values must never be labelled actual expected losses.

2. The IG-Smart Board Assurance Evidence Chain – seven decision stages

Stage	Management must establish	Evidence a board may inspect	Escalation condition
B1. Business service	Critical services, customers, safety and data exposure	Service and dependency inventory; BIA	Unowned consequential service
B2. Threat scenario	Plausible attack path and consequence	Threat modelling, incidents, external intelligence	Credible high-impact scenario not assessed
B3. Control assertion	What protection or recovery is claimed	Control design and accountability	Control not assigned or incorrectly scoped
B4. Verification	Is it implemented and effective?	Tests, internal audit, independent review, age and limitations	Unsupported management confidence
B5. Residual risk	Remaining exposure and tolerance	Risk assessment, exceptions, uncertainty	Tolerance exceeded or cannot be evaluated
B6. Executive decision	Mitigate, transfer, change, tolerate or stop	Options paper, authority and budget	Risk acceptance outside delegation
B7. Continuous oversight	Outcome, dependencies, triggers and escalation	Action tracker, retests, incident and service changes	Overdue critical action or material change

Non-negotiable safeguard: a favourable aggregate dashboard cannot override a material uncontrolled exposure or a statutory obligation. Senior management must own the underlying risk; advisory teams and assurance reviewers must not silently assume that authority.

3. The one-page board cyber assurance pack

A concise front sheet should cover **reporting period, current decision request, material changes since the previous meeting, top three consequential scenarios, exposures outside risk tolerance, significant evidence limitations, actions requiring investment or acceptance, and next review trigger**. A detailed appendix should link to the risk record, test evidence, relevant supplier assessments and incident exercises.

Front-sheet field	Minimum defensible entry	Poor substitute
Decision required	Exact proposed resolution, options and delegated owner	“For noting” when action is needed
Critical exposure	Named service and plausible harm pathway	Severity colour without consequences
Evidence quality	Artefact, date, scope, independent challenge, exceptions	“Audited / compliant” without boundaries
Time to recover	Tested scenario, test date, achieved result vs tolerance	Unsupported RTO from a policy
Supplier dependence	Concentration and credible substitution plan	List of vendors only
Residual risk	Owner, rationale, uncertainty, acceptance authority	A numeric score alone
Follow-up	Decision log, action owner, milestone and retest	“Management will monitor”

Reporting two layers without creating two truths

An **executive layer** explains service consequence, exposure, assurance confidence, decision and funding. The **technical appendix** records findings, scope, dependencies, quantitative assumptions and reproducible evidence. The executive conclusion must not be more confident than the underlying technical record.

4. A defensible risk-to-decision translation

Consider an illustrative high-priority supplier identity-management outage. The service owner maps which customer channels and regulated activities would become unavailable; the CISO maps the plausible attack or failure path; IT verifies recovery performance; the supplier owner confirms dependencies; legal/privacy teams assess notification and contractual obligations; and the CRO tests the acceptability of residual exposure. The board decides whether to fund resilience changes or approve a time-limited, properly authorised exception.

The risk register should show **scenario / exposed service / impacted people / existing controls / evidence confidence / plausible consequence / tolerance / owner / treatment / decision date / next test**. Risks should not be labelled “accepted” merely because no remediation budget exists.

Risk appetite and KRIs

A useful key risk indicator measures **material exposure to a business consequence**, not an activity count. For example: “critical identity infrastructure without a tested secondary recovery path” may be more relevant to a board than “number of backups run”. Board-facing indicators should disclose thresholds, definitions, data sources, measurement period and action upon breach.

Three-lines separation

First-line business and technology owners manage risks and controls; second-line risk/privacy/security governance functions set challenge and oversight arrangements as appropriate; internal audit gives independent assurance under its own mandate. The precise model differs by organisation. The retained virtual CISO may support second-line or first-line functions depending on scope: neither the consultant's title nor an outsourced contract makes assurance automatically independent.

5. A 12-domain board reporting architecture

Domain	Board's question	Examples of evidence	Trigger for deep dive
Critical services	What cannot fail safely?	BIA, services/dependencies	Unknown material service
Governance	Who owns digital risk?	Delegations and committee minutes	Unresolved responsibility
Threat landscape	Which plausible scenarios changed?	Threat intelligence, scenario mapping	New relevant exploitation
Asset visibility	Are critical assets known?	Coverage reconciliation	Unknown externally exposed assets
Identity	Is privileged access controlled?	MFA/PAM control tests	Material privileged access gap
Vulnerability	Are exploitable gaps resolved?	SLA exceptions, validation	Critical untreated exploitable exposure
Supplier risk	Can partners undermine resilience?	Tiering, attestations, independent reviews	Concentration or unverified critical supplier
Data protection	What harm could result from data loss?	DPIAs, incident capability	High-risk processing unmanaged
Response	Can leaders make timely decisions?	Tabletop findings, escalation tests	Executive role confusion
Recovery	Can service be restored to tolerance?	Recovery exercises and dependencies	Untested critical recovery
Assurance	How independent and current is our view?	Audit coverage and exceptions	Scope gap or conflict
People	Can the organisation execute the plan?	Skills, succession, exercises	Single point of failure

6. What assurance levels mean

Management assertion: an accountable owner reports a control exists; valuable but not an independent assessment. **Observed operation:** an artefact or test indicates operation within a defined scope and time. **Independent challenge:** a competent reviewer not conflicted in the subject work examines and reports against criteria. **External certification:** a qualified body certifies against a specified scheme and scope, which does not validate all enterprise cyber risks. Board packs should make these evidence levels explicit.

Avoid stacking impressive badges as a substitute for scope analysis. A current ISO/IEC 27001 certificate is significant if relevant to the system and services assessed, but the scope statement, locations, control boundaries, surveillance status and exceptions still matter.

7. Incident readiness and executive rehearsals

The board should know who can declare a major incident, disconnect services, involve law enforcement, engage specialist counsel, make relevant regulatory notifications, communicate with affected individuals and approve recovery priorities. A tabletop should test **decision rights and trade-offs**, not simply whether the IT team can restore a system.

A good scenario escalates in stages: a supplier compromise; uncertain data access; public reporting; operational downtime; customer and regulator enquiries. Capture the decisions taken, contrary evidence, unresolved role boundaries and post-exercise actions. Report limitations openly: a tabletop does not validate restoration engineering or incident containment.

8. Illustrative board decisions – not actual IG-Smart client events

Scenario A: Ransomware risk at a clinical SaaS provider. A tested restore meets the recovery-time objective but misses data-integrity reconciliation. The pack records recovery confidence as partial, identifies the affected clinical workflow, allocates owners and requests a conditional deployment decision. It does not treat a successful restore as proof of patient safety.

Scenario B: Supplier concentration. Two critical systems rely on the same cloud identity provider. The vendor holds certifications, but the client's own fallback is untested. The board considers a recovery exercise and proportionate alternate access arrangements; vendor certification alone does not remove concentration risk.

Scenario C: Cyber governance leadership vacancy. The company has technical engineers but no clear escalation owner or board-level risk interpretation. A scoped virtual CISO may establish governance continuity and reporting, but management retains accountability and separate audit independence may still be necessary.

9. Executive scrutiny: 15 questions before approving the pack

1. Which decision are you asking us to make today?
2. Which essential service and customer outcome underpin this risk?
3. What is different since last quarter?
4. Which assumptions make the conclusion uncertain?
5. What evidence is independent and within scope?
6. Which report findings remain unresolved?
7. Which threats or failures were not considered?
8. What would invalidate the current assurance view?
9. Which supplier or fourth party could undermine recovery?
10. Have the most consequential recovery paths been tested?
11. Which risk exceeds approved tolerance?
12. Who owns the action and who can authorise acceptance?
13. What happens if the proposed funding is declined?
14. How does legal, privacy or clinical risk alter the decision?
15. What new evidence will return to this committee?

10. Original board decision briefing – reusable text

Decision sought: [specific resolution]; **Service and population affected:** [description]; **Relevant scenario:** [events and path to consequence]; **Current safeguards and verification:** [source, scope, test date, exceptions]; **Residual exposure:** [risk and confidence]; **Options:** [A/B/C with estimated resources, assumptions and drawbacks]; **Recommendation:** [rationale and remaining limitations]; **Approving authority:** [delegation]; **Follow-up:** [owner, date, objective verification]; **Change trigger:** [incident, supplier, architecture, regulatory change].

No board member should be asked to accept a red/amber/green status in place of this underlying decision record.

11. Common buyer questions

Does the board need technical vulnerability lists? Usually only the subset needed to explain material exposure; preserve detailed evidence in a controlled appendix.

Can a board rely on a penetration test? It offers bounded point-in-time evidence, not proof that all risks or recovery dependencies are controlled.

Is the UK Cyber Governance Code legislation? It is a government Code of Practice offering governance actions; confirm independently whether a particular statutory, contractual or sector-specific requirement applies to the organisation.

Can an external vCISO report independently on controls they helped implement? An adviser can describe implementation and monitor outcomes; a formal independent assurance opinion requires conflict evaluation and suitable separation.

How often should the pack be updated? Set a proportionate routine cadence with material change triggers, including incidents, supplier shifts and critical test failures.

Does a financial risk estimate establish likelihood? Not unless its assumptions and model are defensible. Avoid implying precision unsupported by data.

A decision-ready board minute: illustrative example

Decision: fund a repeat recovery exercise before extending a critical supplier dependency. **Evidence:** the last exercise did not demonstrate the recovery time management had assumed; the affected service and test limitations are stated. **Unknown:** whether the revised configuration resolves the failure. **Options:** limit further dependency, commission the retest, or adopt a documented alternative. **Owner:** the accountable business-service executive. **Return to the board:** test result, unresolved exceptions and the consequences for the service decision.

This example does not assert an actual incident, client outcome or measured financial loss. Its value is the link between a claim, contrary evidence, a choice and accountable follow-up. A green dashboard without those links would be less informative.

12. How to use the framework

Start with one consequential service and one upcoming board decision, not an enterprise-wide dashboard rebuild. Inventory current management claims, find inspectable evidence, identify exceptions and responsible owners, then test a one-page pack with a board representative. Make the next review depend on outcomes, not simply the next reporting date.

Next step: Talk to a Senior Practitioner about the board's specific reporting, accountability or assurance requirements. No predetermined service deliverable or assurance opinion is implied.

Sources

- [S1] UK Government, Cyber Governance Code of Practice (8 April 2025) <https://www.gov.uk/government/publications/cyber-governance-code-of-practice/cyber-governance-code-of-practice>

- [S2] NCSC, Cyber Security Toolkit for Boards <https://www.ncsc.gov.uk/collection/board-toolkit>
- [S3] NCSC, Principle E: Assurance and Oversight <https://www.ncsc.gov.uk/collection/board-toolkit/principle-e-assurance-and-oversight>
- [S4] NCSC, Board questions and resources <https://www.ncsc.gov.uk/collection/board-toolkit/resources/downloads>