PROTECHT

CYBER RISK OPERATING MODEL SCORECARD

How connected is your cyber risk operating model?

A practical checklist for assessing cyber risk connection across cyber, risk, resilience, compliance and vendor teams. Use this scorecard to identify where your cyber risk program is connected, where gaps remain and which action areas should come next.

PROTECHT

Introduction.

Cyber risk looks manageable until pressure hits: a vulnerability, supplier issue, incident, audit request or board question. At that point, teams need to know what is exposed, who owns it, which controls apply and what evidence can be trusted.

This scorecard helps you assess how well your cyber operating model connects risk, controls, assets, vendors, incidents, evidence and reporting, so you can identify where fragmentation is creating blind spots and which gaps to address first.

It is designed for CISOs, CIOs, cyber risk leaders, CROs, enterprise risk managers, vendor risk teams and compliance leaders who need a clearer view of how cyber risk connects across the organisation.

How to score yourself.

For each statement, select the response that best reflects your current position.

Response	Meaning	Score
Yes	This is consistently in place and working well	2
Partly	This exists, but is inconsistent, informal or not fully embedded	1
No	This is not currently in place	0
Not Sure	You do not have enough visibility to answer confidently	0

Note: "Not sure" scores zero because lack of visibility is itself a sign of fragmentation.

Total possible score: **70 points**

7 sections x 5 statements x 2 points.

PROTECHT

Capability 1: Connect cyber risk to enterprise GRC.

Focus:

Can cyber risk be understood in the context of enterprise risk, resilience, compliance, vendor risk and board reporting?

Statement	Yes	Partly	No	Not Sure
Enterprise risk leaders can see how material cyber risks relate to business objectives, risk appetite and enterprise risk categories.				
Cyber risk reporting explains business impact and priority actions, not only technical activity or control status.				
Operational resilience and business continuity teams can identify which critical services may be affected by material cyber risks or incidents.				
Enterprise risk, compliance and assurance teams can see relevant cyber risks, controls and evidence without requesting separate updates.				
Cyber risk decisions are made with input from the right cyber, risk, resilience, compliance and business stakeholders, rather than being handled as a standalone technical process.				

Reflection prompt

Where does cyber risk still sit outside your enterprise risk or governance processes?

Notes:

Action prompt

Identify one cyber risk that should be connected to enterprise risk, resilience, compliance or board reporting but is not currently linked.

Action:

PROTECHT

Capability 2: Understand assets, vendors and critical dependencies.

Focus:

Can you see what matters most, where your exposure sits and which third parties may affect critical services?

Statement	Yes	Partly	No	Not Sure
Cyber and risk teams can identify the critical assets, systems, data and vendors that support important business services.				
Asset owners, vendor owners and service owners are clearly recorded and can be found quickly when action is required.				
Teams can see how a material vendor, fourth party, system or asset issue could affect business services, resilience or customer outcomes.				
Vendor cyber assessments and evidence are current enough to support risk decisions, not only onboarding or periodic review.				
When a vulnerability, supplier issue or service disruption occurs, teams can quickly identify what is affected, who owns the response and what evidence is available.				

Reflection prompt

Which critical services depend on vendors or technology assets where visibility is incomplete?

Notes:

Action prompt

Select one critical service and map the key assets, vendors, owners and evidence sources that support it.

Action:

PROTECHT

Capability 3: Link threats, vulnerabilities and exposure.

Focus:
Can emerging threats and vulnerabilities be connected to the assets, services, controls and risks that matter?

Statement	Yes	Partly	No	Not Sure
Cyber and risk teams can see which assets, systems, services or vendors are affected by material threats or vulnerabilities.				
Vulnerability prioritisation reflects asset criticality, business impact and risk exposure, not only technical severity scores.				
Emerging threats can be assessed against existing risks, controls, response plans and assurance evidence.				
Remediation decisions are based on clear ownership, business impact and control effectiveness, not only issue volume.				
When a significant threat or vulnerability emerges, teams can quickly explain what changed, what is exposed, what action is required and who owns it.				

Reflection prompt

Where are threat or vulnerability insights still disconnected from risk and business impact?

Notes:

Action prompt

Choose one recent vulnerability or threat and test whether it can be traced to assets, risks, controls, owners and actions.

Action:

PROTECHT

Capability 4: Reduce control and framework duplication.

Focus:
Are controls mapped across frameworks, obligations and assurance activities, or are teams repeating work?

Statement	Yes	Partly	No	Not Sure
Teams can identify where the same or similar cyber controls support multiple frameworks, obligations or assurance needs.				
Control owners can see which frameworks, risks, obligations and evidence requirements relate to the controls they manage.				
Evidence collected for one control can be reused across relevant frameworks, audits or reporting requests without repeated manual collection.				
Assurance, compliance and cyber teams can see whether key controls are designed, operating and evidenced without maintaining separate versions of the same control.				
When a framework, obligation or control requirement changes, teams can identify which controls, evidence, owners and reports are affected.				

Reflection prompt

Where does the same control or evidence get recreated for different frameworks, audits or stakeholders?

Notes:

Action prompt

Identify one high-effort control area and assess whether evidence could be reused across multiple obligations.

Action:

PROTECHT

Capability 5: Strengthen incident readiness and enterprise response.

Focus:
Can incidents be captured, escalated, linked and explained in a way that supports both cyber response and enterprise decision-making?

Statement	Yes	Partly	No	Not Sure
Cyber incidents are captured in a consistent, structured way that supports investigation, escalation, reporting and lessons learned.				
Response teams can quickly identify affected assets, vendors, controls, risks, obligations and business services during an incident.				
Incident owners, action owners and escalation paths are clear enough to coordinate response without relying on informal follow-up.				
Evidence collected during an incident can support executive updates, assurance reviews, regulatory reporting and post-incident improvement.				
Lessons learned from incidents are translated into updated controls, processes, resilience plans or risk assessments.				

Reflection prompt

During an incident, where would teams still need to chase facts manually?

Notes:

Action prompt

Review a recent incident or exercise and identify which links were missing: assets, controls, vendors, obligations, owners, evidence or actions.

Action:

PROTECHT

Capability 6: Prove assurance and compliance.

Focus:
Can the organisation demonstrate control effectiveness, compliance status and resilience using current evidence?

Statement	Yes	Partly	No	Not Sure
Teams can quickly find current evidence for the cyber controls, risks, obligations or assurance activities they need to support.				
Assurance activities are tracked through to outcomes, findings, issues and remediation actions.				
Control gaps, audit findings and remediation actions can be traced back to the risks, obligations, assets or services they affect.				
Compliance status can be reported from connected evidence and assurance data, rather than manually reconciled from spreadsheets or separate systems.				
Executives, auditors or regulators can be given a clear, evidence-backed view of cyber resilience without requiring a last-minute evidence hunt.				

Reflection prompt

Where is evidence still scattered across spreadsheets, screenshots, inboxes or disconnected systems?

Notes:

Action prompt

Pick one important obligation or control and test whether evidence can be found quickly, traced to an owner and linked to assurance status.

Action:

PROTECHT

Capability 7: Report cyber risk with confidence.

Focus:
Can cyber posture be communicated in a way executives, boards, auditors and regulators can understand and act on?

Statement	Yes	Partly	No	Not Sure
Executives can see the current cyber risk posture, priority issues and required actions without relying on manually assembled updates.				
Cyber reporting explains what matters, why it matters, what has changed and what action is required.				
Board, regulator and audit reporting is based on trusted, current and connected cyber risk, control, incident, vendor and assurance data.				
Cyber reports show trends, emerging risks, overdue actions, control gaps and changes in exposure in business-relevant terms.				
Leaders can use cyber risk reporting to make decisions about investment, prioritisation, resilience and risk acceptance.				

Reflection prompt

Where does cyber reporting still depend on manual interpretation or last-minute narrative building?

Notes:

Action prompt

Review your latest cyber report and identify whether it clearly explains posture, exposure, assurance, action and business impact.

Action:

PROTECHT

Score interpretation.

Score	Interpretation	Priority Focus
0–20 Fragmented and reactive	Your cyber risk operating model is likely fragmented. Cyber activity, evidence, ownership and reporting may sit across different systems and teams, making it difficult to understand exposure or prove assurance under pressure.	Start by connecting your highest-priority cyber risks to assets, controls, vendors, obligations and evidence.
21–40 Foundations in place, but disconnected	You have important building blocks, but they may not be consistently connected across cyber and enterprise GRC. Reporting may still require manual consolidation, and assurance may depend on effort from key individuals rather than a repeatable model.	Connect cyber activity to enterprise risk, resilience, vendor risk, compliance and assurance workflows.
41–55 Maturing, with integration gaps	Your organisation has a maturing cyber risk operating model. Key elements are likely in place, but some areas may still be inconsistent, duplicated or disconnected from business impact and enterprise reporting.	Improve evidence reuse, vendor dependency visibility, control mapping and executive-ready reporting.
56–70 Connected and assurance-ready	Your cyber risk operating model is well connected. You have strong visibility across cyber risk, assets, controls, incidents, vendors, evidence and reporting, and cyber is likely integrated into broader enterprise risk and governance processes.	Continue improving automation, continuous assurance, AI-supported insight and optimisation across cyber and GRC workflows.

PROTECHT

Priority action planner.

After calculating their score, readers should identify:

Lowest-scoring section

Our lowest-scoring section is:

- Cyber risk and enterprise GRC
- Assets, vendors and dependencies
- Threats, vulnerabilities and exposure
- Controls and frameworks
- Incident readiness and response
- Assurance and compliance
- Reporting and confidence

Biggest blind spot

The question we struggle to answer the most is:

- What is affected?
- Who owns it?
- What controls apply?
- What evidence do we have?
- Which vendors are involved?
- What is the business impact?
- What do we tell the board or regulator?

First 30-day action

Our first 30-day action is:

Examples:

- Map one critical service to its assets, vendors and controls.
- Rationalise duplicate controls across two frameworks.
- Link one key cyber risk to enterprise risk appetite.
- Review one incident and identify missing evidence links.
- Create a clearer board-level cyber risk narrative.
- Test whether vendor evidence can be collected and assessed more efficiently.