OUTLIERS RISK MANAGEMENT CENTRE™

Cyber Risk Toolkit™

Govern, detect, respond to and recover from cyber risk

CISO / IT / CRO · Access Tier T2 · Flagship Edition 2026

Publication-ready resource for the Outliers Resource Library

1. Full Guide

Cyber risk threatens confidentiality, integrity and availability of information and operations. This toolkit applies the Identify–Protect–Detect–Respond–Recover lifecycle with governance, control maturity, incident response and resilience.

The cyber lifecycle

Function	Focus
Identify	Asset & data inventory; risk assessment
Protect	Access control, MFA, patching, encryption, training
Detect	Monitoring, logging, threat detection
Respond	Incident response plan, containment, comms
Recover	Backups, restoration, lessons learned

Maturity model

L1 Fragile	L2 Functional	L3 Disciplined	L4 Strategic	L5 Resilient
Informal / reactive	Basic, siloed	Standardised & governed	Integrated & quantified	Predictive & embedded

2. Templates

2.1 Cyber risk register (sample)

Working register: Cyber_Risk_Register.xlsx. Sample:

ID	Category	Risk	Score	Rating	Key control
CR-001	Ransomware	Encrypts production systems	15	Critical	EDR; immutable backups
CR-002	Phishing	Credential theft / takeover	16	Critical	MFA everywhere
CR-003	Data breach	Customer PII exposure	10	High	Access control; DLP

2.2 Cyber incident response playbook (steps)

1. Detect & triage (severity classification)
2. Activate IR team & roles
3. Contain (isolate affected systems)
4. Eradicate (remove threat, patch)
5. Recover (restore from clean backups)
6. Notify (regulators/customers as required)
7. Review (post-incident lessons)

2.3 Cyber risk scorecard (control maturity)

Control domain	Maturity (1-5)	Target
Access & identity (MFA)	3	5
Patch & vulnerability mgmt	3	4
Backup & recovery	3	5
Monitoring & detection	2	4
Awareness & training	3	4

3. Registers

Use the Cyber Risk Register with the Incident Register (XLSX) to log security incidents, severity and resolution.

4. Checklists

Cyber readiness checklist

- ☐ Critical assets and data inventoried
- ☐ MFA enforced on all systems
- ☐ Patch SLA defined and met for criticals
- ☐ Immutable, tested backups
- ☐ 24/7 monitoring / detection capability
- ☐ Incident response plan documented and tested
- ☐ Third-party/vendor cyber due-diligence
- ☐ Security awareness training delivered
- ☐ Board cyber reporting in place

Governance Structure

Risk is governed through three lines of defence under board oversight:

Layer	Role	Responsibility
Board	Oversight	Approves policy, appetite; oversees the risk profile
Risk / Audit Committee	Focused oversight	Reviews top risks, appetite, assurance
1st line — Management/owners	Own & manage	Identify, assess, control and report risk in operations
2nd line — Risk/Compliance	Oversee & challenge	Set framework, monitor, challenge, aggregate reporting
3rd line — Internal Audit	Assure	Independent assurance over the risk and control system

Reporting Templates

Standard cyber report structure

- Executive summary & key messages
- Profile vs appetite (RAG)
- Top risks & movement
- KRIs and breaches
- Incidents & losses in period
- Actions & overdue items
- Decisions / escalations sought

KRI reporting table (example)

KRI	Current	Threshold	RAG	Trend	Action
Open critical vulnerabilities	1	0	Red	Down	Emergency patch
Critical patch SLA	91%	≥95%	Amber	Up	Improve cadence
Security incidents (severe)	0	0	Green	Stable	Maintain
Backup restore test	Pass	Pass	Green	Stable	Maintain

Board Reporting Example

Illustrative one-page board summary (replace with live data):

Item	Status	Commentary

Cyber posture	**Amber**	1 critical vulnerability open; MFA rollout 85% complete
Incidents	**Green**	No severe incidents this period; one phishing attempt contained
Resilience	**Green**	Backup restore test passed
Decisions sought	—	Approve funding for 24/7 monitoring

Disclaimer

This toolkit is a professional management resource, not legal, regulatory or audit advice. Calibrate scoring scales, appetite, limits and governance to your organisation, sector and applicable regulation. Sector-specific requirements (e.g. prudential, data-protection, HSE) must be confirmed against current local regulation.