



SAMPLE RISK REGISTER

Cybersecurity Risk Register

A structured view of material risks, risk ownership, treatment plans, and decisions that leadership can understand and act on.

Cybersecurity Risk Register

A working record of material cybersecurity risks, business impact, existing controls, risk treatment, ownership, and management decisions.

Risk method

Likelihood and impact are assessed on a 1-5 scale. Inherent risk is assessed before listed controls; residual risk reflects the remaining exposure after current controls and approved treatment plans.

Portfolio snapshot

Open risks	High / critical	Treatment plans	Overdue actions
8	3	5	1
Current register	Leadership attention	Active or planned	Owner follow-up

Current risk register

Risk	Asset / process	Likelihood	Impact	Inherent	Key controls	Residual	Owner	Treatment / due	Status
Compromise of cloud identity account	Identity / access	4	5	Critical	MFA; least privilege; access reviews	High	Operations Lead	Expand MFA coverage Oct 21	In progress
Unauthorized exposure of customer data	Cloud storage / SaaS	3	5	High	Access control; data handling policy; vendor reviews	Medium	Engineering Lead	Review permissions Oct 11	In progress
Ransomware disrupts business operations	Endpoints / file storage	3	5	High	Managed backups; endpoint protection; response plan	Medium	IT Provider	Run restore test Nov 15	Planned
Phishing leads to account takeover	Email / workforce	4	4	High	Awareness training; MFA; simulations	Medium	Security Owner	Targeted refresher Dec 12	Active
Critical vendor outage affects service delivery	Vendor management	3	4	High	Vendor review; backup process; contractual review	Medium	Operations Lead	Assess recovery options Nov 30	Open
Unapproved AI tool receives company data	Data handling / AI use	3	4	High	AI policy; training; approved-tool list	Medium	Executive Sponsor	Publish AI policy Oct 31	In progress
Privileged access not removed after offboarding	Joiner / mover / leaver	2	5	High	Offboarding checklist; periodic review	Low	HR + IT	Validate evidence Oct 18	Open
Security incident is escalated too slowly	Incident response	2	4	Medium	IR plan; contact tree; tabletop exercise	Low	Security Owner	Run tabletop Nov 15	Planned

Risk decision notes

Leadership attention

The highest residual risks relate to cloud identity and customer-data access. The recommended course is to complete the defined remediation actions, validate evidence, and formally accept only those residual risks that remain proportionate to business needs.

Evidence retained

Evidence	Examples
Risk assessment record	Scoring rationale, risk owner, treatment decision, review date
Control evidence	Access review records, policy acknowledgements, configuration evidence, test outcomes
Exception approval	Business justification, compensating controls, approver, expiry, and planned reassessment
Management review	Monthly risk-review notes and quarterly executive report