Aegentra
ACADEMY

ISO/IEC 27001:2022 Risk Register

Worked example with inherent and residual scoring

Likelihood and impact are scored 1–5; score = likelihood × impact. Bands: 1–4 Low, 5–9 Medium, 10–25 High. Each risk maps to the Annex A controls that treat it, which is what an auditor looks for when tracing risk to control.

RISK ID	ASSET / AREA	RISK DESCRIPTION	TYPE	INHERENT LIKELIHOOD	INHERENT IMPACT	INHERENT SCORE	INHERENT RATING	EXISTING CONTROLS / TREATMENT	RESIDUAL LIKELIHOOD	RESIDUAL IMPACT	RESIDUAL SCORE	RESIDUAL RATING	DECISION	RISK OWNER	ANNEX A CONTROLS
R-001	Customer data	Phishing leads to credential compromise of a staff account with customer-data access	Confidentiality	4	4	16	High	Phishing-resistant MFA (FIDO2) for all staff; Conditional Access blocks legacy auth; quarterly simulated phishing	2	3	6	Medium	Treat	Security Lead	A.5.17, A.6.3, A.8.5
R-002	Production platform	Azure regional outage takes the production platform offline beyond the 4-hour RTO	Availability	2	5	10	High	Active-passive across two Azure regions; quarterly failover testing; RTO 4h / RPO 15min	1	4	4	Low	Treat	CTO	A.5.29, A.5.30, A.8.14
R-003	Source code	Secret committed to the repository and exposed	Confidentiality	3	4	12	High	Secret scanning in CI blocks the build; pre-commit hooks; Key Vault for all runtime secrets	1	4	4	Low	Treat	Engineering Lead	A.8.4, A.8.24, A.8.28
R-004	Suppliers	A sub-processor suffers a breach affecting customer data we are accountable for	Confidentiality	3	4	12	High	Security schedule in all supplier contracts; annual review of SOC 2 / ISO 27001 evidence; 24-hour notification clause	2	4	8	Medium	Treat	Security Lead	A.5.19, A.5.20, A.5.21, A.5.22
R-005	Personal information	Eligible data breach not notified to the OAIC within the statutory period	Compliance	2	5	10	High	IR plan includes an NDB assessment step with a 30-day clock; legal counsel on the escalation path	1	5	5	Medium	Treat	Privacy Officer	A.5.24, A.5.26, A.5.34
R-006	Endpoints	Lost or stolen laptop containing cached customer data	Confidentiality	3	3	9	Medium	BitLocker full-disk encryption enforced by Intune; remote wipe; 5-minute screen lock	1	2	2	Low	Treat	IT Lead	A.7.9, A.8.1, A.8.24
R-007	Application	Vulnerability in a third-party dependency exploited in production	Integrity	4	4	16	High	Dependency scanning in CI; 14-day remediation SLA for critical; annual external penetration test	2	3	6	Medium	Treat	Engineering Lead	A.8.8, A.8.29
R-008	Access	Departed employee retains access after termination	Confidentiality	3	4	12	High	HRIS-triggered automated deprovisioning within 1 business day; quarterly access reviews	1	4	4	Low	Treat	IT Lead	A.5.11, A.5.18, A.6.5
R-009	Privileged access	Standing privileged access misused or compromised	Confidentiality	2	5	10	High	Entra PIM just-in-time elevation with approval and time limits; all privileged actions logged to Sentinel	1	4	4	Low	Treat	Security Lead	A.8.2, A.8.18

RISK ID	ASSET / AREA	RISK DESCRIPTION	TYPE	INHERENT LIKELIHOOD	INHERENT IMPACT	INHERENT SCORE	INHERENT RATING	EXISTING CONTROLS / TREATMENT	RESIDUAL LIKELIHOOD	RESIDUAL IMPACT	RESIDUAL SCORE	RESIDUAL RATING	DECISION	RISK OWNER	ANNEX A CONTROLS
R-010	Backups	Ransomware encrypts production data and backups together	Availability	2	5	10	High	Immutable geo-redundant backup; restores tested quarterly; backup credentials isolated from production identity	1	4	4	Low	Treat	CTO	A.8.13, A.8.7
R-011	Compliance	APRA-regulated customer requires CPS 234 evidence we cannot produce	Compliance	3	3	9	Medium	CPS 234 control mapping maintained; evidence pack refreshed quarterly	1	3	3	Low	Treat	Security Lead	A.5.31, A.5.36
R-012	Insider	Staff member exfiltrates customer data before resigning	Confidentiality	2	4	8	Medium	Purview DLP on customer data; anomalous-download alerting in Sentinel; background checks for privileged roles	1	4	4	Low	Treat	Security Lead	A.6.1, A.8.12, A.8.16
R-013	Change	Untested production change causes a customer-visible outage	Availability	3	3	9	Medium	Peer-reviewed pull requests; automated test gate; documented rollback for every release	2	2	4	Low	Treat	Engineering Lead	A.8.32
R-014	Shadow IT	Staff process customer data in an unapproved SaaS tool	Confidentiality	3	3	9	Medium	Defender for Cloud Apps discovery; approved-tools register; acceptable use training	2	3	6	Medium	Treat	Security Lead	A.5.23, A.8.19
R-015	Physical	Unauthorised access to the Melbourne office	Confidentiality	2	2	4	Low	Swipe-card entry with logging; visitors escorted; clear desk policy	1	2	2	Low	Accept	Office Manager	A.7.1, A.7.2, A.7.6
R-016	Certification	Major nonconformity at Stage 2 delays certification and a customer contract	Compliance	3	4	12	High	Internal audit before Stage 1; management review; gap remediation tracked to closure	1	4	4	Low	Treat	ISMS Owner	A.5.35, A.5.36
R-017	Logging	Insufficient logging prevents reconstruction of an incident	Integrity	2	4	8	Medium	Centralised logging in Sentinel with 12-month immutable retention; detection coverage mapped to MITRE ATT&CK	1	3	3	Low	Treat	Security Lead	A.8.15, A.8.16, A.8.17
R-018	Awareness	Staff unaware of security obligations, increasing susceptibility to social engineering	Confidentiality	3	3	9	Medium	Induction plus annual training; quarterly phishing simulation with targeted follow-up	2	3	6	Medium	Treat	Security Lead	A.6.3
R-019															
R-020															
R-021															

RISK ID	ASSET / AREA	RISK DESCRIPTION	TYPE	INHERENT LIKELIHOOD	INHERENT IMPACT	INHERENT SCORE	INHERENT RATING	EXISTING CONTROLS / TREATMENT	RESIDUAL LIKELIHOOD	RESIDUAL IMPACT	RESIDUAL SCORE	RESIDUAL RATING	DECISION	RISK OWNER	ANNEX A CONTROLS
R-022															
R-023															
R-024															
R-025															