Aegentra
ACADEMY

ISO/IEC 27005:2022 Information Security Risk Assessment Worksheet

Asset → threat → vulnerability → control → likelihood → consequence → treatment → residual

ISO 27001 Clause 6.1.2 requires a documented information security risk assessment process but does not mandate which one — ISO/IEC 27005 is the usual choice, and this is what it produces. Twelve worked risks for an Australian B2B SaaS. Treatment options follow ISO 27005: modify, retain, avoid or share.

REF	ASSET	ASSET OWNER	THREAT	VULNERABILITY	EXISTING CONTROLS	LIKELIHOOD	CONSEQUENCE	RISK LEVEL	ABOVE CRITERIA?	TREATMENT OPTION	TREATMENT DETAIL	RESIDUAL LIKELIHOOD	RESIDUAL CONSEQUENCE	RESIDUAL LEVEL	RISK OWNER
R-01	Customer database (Azure SQL)	CTO	Credential compromise of a privileged account	Legacy authentication still enabled on two service accounts	Phishing-resistant MFA for staff; Conditional Access; quarterly access review	4	5	20	Yes	Modify	Disable legacy auth; move service accounts to managed identities; enforce MFA with no exclusions	2	5	10	CTO
R-02	Customer database	CTO	Ransomware encrypts production and backups	Backup immutability never verified by test	Immutable offsite backups; EDR on all endpoints; annual restore test	3	5	15	Yes	Modify	Attempt deletion from a compromised admin account during the next restore test; document the result	2	4	8	CTO
R-03	Source code repository	Head of Engineering	Insider exfiltration of intellectual property	No egress monitoring on developer workstations	Role-based repo access; signed commits; offboarding checklist	2	4	8	Yes	Modify	Enable repository audit logging with alerting on bulk clone; add IP clause to contractor agreements	2	3	6	Head of Engineering
R-04	Microsoft 365 tenant	IT Manager	Business email compromise leading to fraudulent payment	Payment approval relies on email confirmation alone	MFA; anti-phishing policy; impersonation protection	3	4	12	Yes	Modify	Require out-of-band verbal verification for any payment detail change above $5,000	2	4	8	CFO
R-05	Production platform	CTO	Regional cloud outage exceeds the contracted RTO	Failover to the secondary region has never been exercised end to end	Active-passive across two Azure regions; documented runbook	2	4	8	Yes	Modify	Run a full failover exercise each half-year and record actual RTO against the 4-hour target	1	4	4	CTO
R-06	Employee personal information (HRIS)	Head of People	Unauthorised internal access to payroll and health data	HRIS permissions granted by role but never reviewed	Role-based access; encryption at rest	3	4	12	Yes	Modify	Quarterly entitlement review with sign-off by the data owner; remove standing admin access	2	3	6	Head of People

REF	ASSET	ASSET OWNER	THREAT	VULNERABILITY	EXISTING CONTROLS	LIKELIHOOD	CONSEQUENCE	RISK LEVEL	ABOVE CRITERIA?	TREATMENT OPTION	TREATMENT DETAIL	RESIDUAL LIKELIHOOD	RESIDUAL CONSEQUENCE	RESIDUAL LEVEL	RISK OWNER
R-07	Third-party support desk	COO	Sub-processor breach exposes customer support content	Contract lacks a defined breach-notification window	Data processing agreement; annual vendor review	2	4	8	Yes	Share	Amend the contract to require notification within 24 hours; add a right to audit	2	3	6	COO
R-08	Corporate laptops	IT Manager	Device loss or theft exposing local data	Full-disk encryption not enforced on contractor devices	Intune compliance policy for staff devices; remote wipe	3	3	9	Yes	Modify	Extend Intune enrolment to contractors or block non-compliant devices from corporate data	2	2	4	IT Manager
R-09	Marketing website	Head of Marketing	**Defacement or malicious script injection**	CMS plugins updated manually and irregularly	WAF; daily backups; least-privilege CMS roles	2	2	4	No	Retain	Within criteria — monitor. Reassess if the site begins handling personal information	2	2	4	Head of Marketing
R-10	Legacy on-premise file server	IT Manager	Unpatched operating system exploited from the internal network	Server is out of vendor support and cannot be patched	Network segmentation; no inbound internet access	3	4	12	Yes	Avoid	Migrate the remaining shares to SharePoint and decommission the server this quarter	1	4	4	IT Manager
R-11	Customer API keys	Head of Engineering	Key leakage through source control or logs	No automated secret scanning in the CI pipeline	Keys stored in Key Vault; rotation documented	3	4	12	Yes	Modify	Enable secret scanning and push protection on all repositories; enforce 90-day rotation	2	3	6	Head of Engineering
R-12	Board and strategy documents	CEO	Unauthorised disclosure of commercially sensitive material	Shared via personal cloud accounts by some directors	Sensitivity labels available but not enforced	2	4	8	Yes	Modify	Enforce sensitivity labels on board content; provide a governed portal and withdraw personal-account sharing	1	4	4	CEO