Aegentra
ACADEMY

Information Security Risk Criteria and Acceptance Criteria

The ISO 27001 Clause 6.1.2 artefact, scored across confidentiality, integrity and availability

Clause 6.1.2 requires risk criteria — including acceptance criteria — to be defined BEFORE anything is assessed. Skipping it leaves "acceptable" to be argued case by case once the numbers are already on the page. This is the document an ISO 27001 auditor asks for first, and almost nobody publishes a worked version.

SCALE	LEVEL	LABEL	DEFINITION — USE THE BAND, NOT THE ADJECTIVE	WORKED INDICATOR
Likelihood	5	Almost certain	Expected to occur more than once a year; has occurred multiple times in the last 3 years	>1 per year
Likelihood	4	Likely	Expected about once a year; has occurred in the last 3 years	~1 per year
Likelihood	3	Possible	Could occur about once in 3 years; has occurred in the sector recently	~1 in 3 years
Likelihood	2	Unlikely	Could occur about once in 10 years; known in the sector	~1 in 10 years
Likelihood	1	Rare	Less than once in 25 years; no known occurrence in the sector	<1 in 25 years
Consequence — Confidentiality	5	Severe	Unauthorised disclosure of sensitive personal information or regulated data at scale	Eligible data breach; OAIC notification required
Consequence — Confidentiality	4	Major	Disclosure of personal information affecting a defined group	Assessment under the NDB scheme required
Consequence — Confidentiality	3	Moderate	Internal-only disclosure beyond need-to-know	Logged; access revoked; no external notification
Consequence — Confidentiality	2	Minor	Disclosure of non-sensitive internal information	Handled by the security team
Consequence — Confidentiality	1	Insignificant	No disclosure of information of value	Noted and closed
Consequence — Integrity	5	Severe	Undetected corruption of customer or financial data affecting decisions or reporting	Restatement or customer remediation required
Consequence — Integrity	4	Major	Detected corruption requiring restore from backup across a critical system	Restore executed; customers notified
Consequence — Integrity	3	Moderate	Localised data error corrected within the working day	Corrected from source
Consequence — Integrity	2	Minor	Isolated record error with no downstream effect	Corrected in place
Consequence — Integrity	1	Insignificant	No measurable integrity impact	No action
Consequence — Availability	5	Severe	Critical service unavailable beyond the maximum tolerable period	Contracted RTO breached on a critical service
Consequence — Availability	4	Major	Critical service degraded for an extended period; SLA credits triggered	SLA breach
Consequence — Availability	3	Moderate	Non-critical service disrupted; workaround available	Workaround in use
Consequence — Availability	2	Minor	Brief degradation; users largely unaffected	Absorbed by capacity
Consequence — Availability	1	Insignificant	No noticeable service impact	No user impact
Acceptance criteria	Extreme (17-25)	Never accept	Treatment mandatory. Cannot be retained. Escalate to the executive immediately and report to the board.	Treatment plan required before the next management review
Acceptance criteria	High (10-16)	Treat	Treatment required with a named owner and a target date. Retention needs written executive approval with an expiry.	Reviewed monthly until residual is Medium or lower
Acceptance criteria	Medium (5-9)	Treat or retain	Retain only where treatment cost is disproportionate to the reduction, with the reasoning recorded.	Reviewed quarterly
Acceptance criteria	Low (1-4)	Retain	Accepted by the risk owner. No treatment required.	Reviewed annually
Acceptance criteria	Any level involving personal information	Escalate	Any risk with a confidentiality consequence of 4 or 5 involving personal information is escalated regardless of likelihood.	Privacy Officer notified; assessed against the NDB scheme