SECURITY RISK ASSESSMENT

Security Risk Assessment and Risk Register

Template

Prepared by Salam Khan, 9T5 Pty Ltd
Founder, cirmp AI
salam@9t5.com.au | cirmpai.au | salamkhan.au
Date: 5 June 2026 | Status: Template

Template. Generic. Complete per engagement.

Document control

Field	Detail
Document title	Security Risk Assessment and Risk Register
Organisation	[Organisation name]
Version	[Version]
Status	[Draft / Final]
Author	[Author, role]
Reviewer	[Reviewer, role]
Contributors	[Contributors]
Approver	[Approver]
Date	[Date]
Next review	[Review cycle, or on material change]
Classification	[Classification]

1. How to use this template

This template is a reusable shell for a security risk assessment and the register that sits under it. Replace every bracketed placeholder with content for the engagement, then delete the greyed example rows. Work through it in order:

1. **Scope it.** Name the systems, data and boundaries the assessment covers, and what is out of scope.
2. **List the risks.** Capture each risk scenario in plain language: the threat and the consequence it would cause.
3. **Score likelihood by impact.** Rate each risk for how likely it is (L) and how serious the impact would be (I), then read the overall rating off the matrix in section 2.
4. **Treat.** Decide the response for each risk: accept, monitor, or a planned treatment. Record the action.
5. **Own.** Assign a single accountable owner to every risk and every treatment.
6. **Review.** Set a review cadence and revisit ratings as controls and the environment change.

The same register travels to delivery and project risk too. The likelihood by impact scoring, the owner column and the treatment column work the same way for a programme risk log as they do for a security one.

2. Methodology

The assessment uses a likelihood by impact approach consistent with ISO 27005 and NIST SP 800-30. Each risk is rated for how likely the scenario is and how serious the impact would be if it occurred. The two scores combine on a five by five matrix to give an overall rating of Low, Medium, High or Critical.

Inherent rating reflects risk before planned treatment, judged against the controls already in place. Residual rating reflects the expected risk once the recommended treatment is delivered and operating.

Likelihood scale

Score	Level	Description
1	Rare	Not expected in normal conditions. Would require an unusual chain of events.
2	Unlikely	Could occur but is not expected. No recent precedent.
3	Possible	Might occur at some point. Seen across the sector.
4	Likely	Expected to occur in most years given current exposure.
5	Almost certain	Expected to occur often, or already occurring.

Impact scale

Score	Level	Description
1	Insignificant	Minor disruption. No data exposure. Handled within business as usual.
2	Minor	Short disruption to a single service. Limited or no sensitive data exposure. Negligible financial cost.
3	Moderate	Service outage or limited exposure of personal data. Some financial cost. Reportable internally.
4	Major	Loss or exposure of sensitive data, or extended outage. Material financial cost. Likely notifiable, with legal or regulatory attention.
5	Severe	Large scale data breach or sustained outage. Significant financial loss, legal or regulatory action, and lasting reputational harm.

Risk matrix (likelihood by impact)

Likelihood / Impact	1 Insig.	2 Minor	3 Moderate	4 Major	5 Severe
5 Almost certain	Med	High	High	Critical	Critical
4 Likely	Low	Med	High	High	Critical
3 Possible	Low	Med	Med	High	High
2 Unlikely	Low	Low	Med	Med	High
1 Rare	Low	Low	Low	Low	Med

Overall rating bands

Rating	Score range	Response expectation
Low	1 to 4	Accept and monitor. No action beyond normal control operation.
Medium	5 to 9	Treat in a planned way. Track to closure at owner level.
High	10 to 16	Treat with priority. Senior oversight. Time bound action.
Critical	17 to 25	Immediate action. Escalate to the governance committee.

3. Risk register

Likelihood (L) and Impact (I) scored 1 to 5. Inherent rating reflects current controls. Residual rating assumes the recommended treatment is delivered and operating. The two greyed rows are examples; replace or delete them, then complete the empty rows.

ID	Asset / system	Risk scenario	Existing controls	L	I	Inherent	Treatment / action	Residual	Owner	Priority
R01	*[system]*	*[describe the threat and its consequence]*	*[what is already in place]*	*L*	*I*	*[rating]*	*[recommended action]*	*[expected rating]*	*[owner]*	*[P1/P2/P3]*
R02	*[system]*	*[describe the threat and its consequence]*	*[what is already in place]*	*L*	*I*	*[rating]*	*[recommended action]*	*[expected rating]*	*[owner]*	*[P1/P2/P3]*
R03										
R04										
R05										
R06										
R07										
R08										
R09										
R10										
R11										
R12										

4. Remediation roadmap

Group treatments into priority waves. Waves describe ordering, not fixed calendar dates. Each wave should complete before the next is fully resourced, though some work runs in parallel. Record the focus and the risk IDs addressed under each wave.

Wave	Focus	Risks addressed	Why this wave
Immediate			
Immediate			
Near term			
Near term			
Planned			
Planned			

5. Residual risk and sign-off

State the expected residual risk position once the recommended treatments are delivered and operating. Note which risks are recommended for acceptance and why, and the review cadence.

Residual risk statement:

Sign-off

By signing, the parties below acknowledge the residual risk position and accept the risks recommended for acceptance, subject to delivery of the treatment plan.

Role	Name	Date	Signature
Risk owner			
CISO or equivalent			
Governance committee			