Cybersecurity Risk Register Template

18 Nov 2025 / Daniel Reeves

Complete

Score	12 / 17 (70.59%)	Flagged items	1	Actions	1

Name of inspector	Daniel Reeves
Position / role	Information Security Analyst
Department or business unit	IT & Cybersecurity
Date of assessment	18.11.2025
Location / site	8 Chifley Square, Sydney NSW 2000, Australia (-33.8664808, 151.2112368)
System or scope being assessed	Enterprise Network Infrastructure
Applicable frameworks	NIST SP 800-30

The next section contains the risk register. Complete one row per identified cyber risk. Score Likelihood (1-5) and Impact (1-5) and manually multiply to get the Inherent Risk Score. Risk rating bands: 1-6 Low, 7-14 Medium, 15-25 High/Critical.

Document existing controls in the Current Controls column and recalculate to get the Residual Risk Score. Assign a named Risk Owner and a Treatment Option. Set a Review Date - High/Critical risks should be reviewed quarterly at minimum.

Flagged items & Actions

1 flagged, 1 action

Flagged items

1 flagged, 1 action

Section 2: Escalation Gates

Is every risk with an Inherent Risk Score of 15 or above assigned to a named owner with a documented treatment option?

No

To do | Assignee: SafetyCulture Staff | Priority: High | Due: 22.06.2026 16:06 PST | Created by: SafetyCulture Staff

Notify people in charge

No. CR-001 and CR-002 both hit 15+ but neither has a named owner or treatment option on record yet.

Other actions

0 actions

Section 1: Cybersecurity Risk Register

4 / 8 (50%)

	Risk ID	Risk Category	Risk Description	Likelihood (1-5)	Impact (1-5)	Inherent Risk Score	Current Controls	Residual Risk Score	Risk Owner	Treatment Option	Review Date
1	CR-001	Access Control	Unauthorized access to enterprise network due to weak multi-factor authentication enforcement across remote users	4	5	20					
2	CR-002	Ransomware	Ransomware infection via phishing email targeting finance department staff with access to critical systems	3	5	15					
3	CR-003	Data Breach	Sensitive employee and customer data exposed due to misconfigured cloud storage permissions on AWS S3 buckets	3	4	12					
4	CR-004	Third Party	Vendor with privileged system access lacking adequate security controls, creating a supply chain vulnerability	3	4	12					

Section 2: Escalation Gates	1 flagged, 1 action, 2 / 3 (66.67%)
Is every risk with an Inherent Risk Score of 15 or above assigned to a named owner with a documented treatment option?	No

To do | Assignee: SafetyCulture Staff | Priority: High | Due: 22.06.2026 16:06 PST | Created by: SafetyCulture Staff

Notify people in charge

No. CR-001 and CR-002 both hit 15+ but neither has a named owner or treatment option on record yet.

Is every risk with a Residual Risk Score of 15 or above escalated to the CISO or senior leadership and documented?	N/A
Does every entry in the register have a Residual Risk Score recorded?	Yes
Does every open risk have a Review Date set?	Yes

Section 3: NIST CSF and ISO 27001 Alignment

5 / 5 (100%)

Confirm that this register's structure and outputs are consistent with the requirements of applicable frameworks. These questions verify that documented risk identification, scoring, treatment and review records are in place to support audit readiness under ISO/IEC 27001:2022 and NIST CSF 2.0.

Does every entry include a named risk owner in line with ISO/IEC 27001:2022 Clause 6.1.2 accountability requirements?	Yes
Is a treatment option (mitigate, accept, transfer or avoid) recorded for every entry in line with ISO/IEC 27001:2022 Clause 6.1.3?	Yes
Is a residual risk score recorded for every entry after controls are applied, in line with ISO/IEC 27001:2022 Clause 8.3?	Yes
Are both inherent and residual risk scores recorded for every entry, consistent with NIST CSF 2.0 and NISTIR 8286 documentation recommendations?	Yes
Is the risk register reviewed and updated on a defined cadence consistent with NIST CSF 2.0 Govern function (GV.OC) and ISO/IEC 27001:2022 Clause 10.1 continual improvement requirements?	Yes

Completion

Before signing, check all rows in the risk register. Confirm no current controls, residual risk scores, risk owners or treatment options are missing. Confirm all risks with a residual score of 15 or above are escalated and documented.

Sections 2 and 3 responses are auto-saved and flagged items are captured automatically. Review any flagged items before signing. The completed register is an audit evidence document. It records the risk management process and does not constitute certification of compliance with any framework.

Inspector sign-off

Daniel Reeves
15.06.2026 16:07 PST

CISO / supervisor sign-off

Margaret Liu
15.06.2026 16:07 PST