ISO 27001 Risk Treatment Plan Template

8 Jan 2026 / RTP-2026-001 / Regina Gonzales

Complete

Score	17 / 26 (65.39%)	Flagged items	1	Actions	0

Inspector Name	Regina Gonzales
Position / Role	Information Security Manager
Date of Assessment	08.01.2026
Location / Site	14 Wingate Rd, Mulgrave NSW 2756, Australia (-33.6204819, 150.834861)
ISMS Scope Covered	Information security management for internal IT systems, data processing, and cloud infrastructure
Assessment Reference No.	RTP-2026-001

The next page contains the risk treatment record. Answer each item based on what you directly observe and document.

One row in the risk record corresponds to one identified information security risk. For each risk, record the treatment decision, map the applicable Annex A controls, assign a named risk owner, set an implementation deadline, and document both the initial and residual risk scores.

Review every row before signing off. If any residual risk score meets or exceeds the escalation threshold, complete the escalation gate questions in Section 2.

Flagged items

1 flagged

Section 2: Residual Risk Escalation Gate

Has a revised treatment action plan been documented for each residual risk above the threshold?

No

RSK-007 currently has no revised treatment plan. Initial mitigation was deemed insufficient but a replacement action plan has not yet been drafted. Assigned owner has been notified. Target completion: 15 July 2026.

Section 1: Risk Treatment Record

4 / 12 (33.33%)

	Risk ID	Risk Description	Treatment Decision (Mitigate / Accept / Transfer / Avoid)	Selected Annex A Controls (reference and title)	Treatment Actions	Risk Owner (named individual)	Implementation Deadline	Implementation Status (Open / In Progress / Closed)	Initial Risk Score	Residual Risk Score	Approval Status (Approved / Pending / Rejected)
1	RSK-001	Unauthorized access to sensitive data due to weak access controls	Mitigate	A.9.1.1 – Access control policy							
2	RSK-002	Data loss from unencrypted storage of confidential information	Mitigate	A.10.1.1 – Policy on the use of cryptographic controls							
3	RSK-003	Third-party vendor with access to internal systems lacks security vetting	Transfer	A.15.1.1 – Information security policy for supplier relationships							
4	RSK-004	Low-likelihood legacy system vulnerability with minimal data exposure	Accept	A.12.6.1 – Management of technical vulnerabilities							

Section 2: Residual Risk Escalation Gate

1 flagged, 4 / 5 (80%)

Complete this section for any risk where the Residual Risk Score equals or exceeds 8. Confirm that appropriate escalation and documentation steps have been taken before sign-off.

Have all risks with a residual score of 8 or above been identified and listed for management review? **NOTE: A residual score at or above 8 indicates treatment actions have not reduced the risk to the organization's accepted tolerance level.**	Yes
Has a named senior owner been assigned to each residual risk that exceeds the threshold?	Yes
Has a revised treatment action plan been documented for each residual risk above the threshold?	No

RSK-007 currently has no revised treatment plan. Initial mitigation was deemed insufficient but a replacement action plan has not yet been drafted. Assigned owner has been notified. Target completion: 15 July 2026.

Have all above-threshold residual risks been formally accepted in writing by an authorized member of senior management?	Yes
Is there a documented timeline for re-assessing residual risks that have been formally accepted rather than further treated?	Yes

Section 3: Statement of Applicability and Documentation Review

9 / 9 (100%)

This section confirms that the Risk Treatment Plan is consistent with ISO 27001 Clause 6.1.3 requirements and is structured to support audit evidence review. Answer each question based on the current state of the completed risk record.

Is the risk assessment methodology used to generate this treatment plan consistent with ISO/IEC 27005?	Yes
Does every row in the risk record correspond to an identified risk from the organization's risk register?	Yes
Has every Annex A control referenced in the risk record been marked as applicable in the Statement of Applicability? **NOTE: Per ISO 27001:2022, the 93 Annex A controls span four themes: Organizational, People, Physical and Technological.**	Yes
Does each row in the risk record include a documented rationale for the treatment option selected?	Yes
Is a named individual, not a team or department, assigned as risk owner for every row?	Yes
Has an implementation deadline been recorded for every treatment action in the record?	Yes
Does the record capture both the initial risk score and the residual risk score for every risk?	Yes
Is there a documented schedule confirming this Risk Treatment Plan will be reviewed at least annually? **NOTE: ISO 27001 Clause 9.3 requires ISMS outputs to be reviewed at planned intervals.**	Yes
Has management formally reviewed and approved the Risk Treatment Plan prior to this assessment being signed off?	Yes

Completion Page

Before signing, review every row in the risk record. Confirm no treatment decisions, owners or due dates are missing. Confirm all risks scored 8 or above have been addressed in Section 2. Flagged responses in Sections 2 and 3 are captured automatically. Review these before signing.

The completed risk record is an audit evidence document. It records the organization's treatment decisions and process. Determination of actual ISO 27001 compliance sits with an accredited certification body.

Inspector name and signature

Regina Gonzales
26.06.2026 16:08 PST

Supervisor / Management approver name and signature

Elroy Shalamontey
26.06.2026 16:08 PST