Risk Assessment Template

Methodology and register aligned with ISO 27001:2022 Clause 6.1

This template provides a practical risk assessment methodology including a likelihood/impact matrix, risk register format, and treatment options. Use it as the foundation for your organisation's information security risk management process.

Prepared by: Nuvencia — Information Security Advisory

Author: Jaouhar Mosbahi, CISSP, CCSP, ISO 27001 LI/LA

Version: 1.0 — February 2026

Classification: Template — Customise for your organisation

This template is provided by Nuvencia for guidance purposes. Organisations should customise it to reflect their specific context, risk appetite, and regulatory requirements.

© 2026 Nuvencia. All rights reserved.

1. Risk Assessment Methodology

This methodology follows a qualitative risk assessment approach using a 5x5 likelihood/impact matrix. Risks are identified by considering threats to information assets, existing vulnerabilities, and the potential business impact of exploitation.

2. Assessment Steps

Step 1: Asset Identification — Identify information assets, their owners, and their value to the organisation.

Step 2: Threat Identification — Identify potential threats to each asset (e.g., cyber attack, human error, natural disaster).

Step 3: Vulnerability Assessment — Identify weaknesses that could be exploited by threats.

Step 4: Likelihood Assessment — Rate the probability of each threat exploiting a vulnerability (1-5 scale).

Step 5: Impact Assessment — Rate the potential business impact if the risk materialises (1-5 scale).

Step 6: Risk Calculation — Risk Score = Likelihood x Impact. Classify as Low/Medium/High/Critical.

Step 7: Risk Treatment — Select treatment option: Mitigate, Transfer, Accept, or Avoid.

Step 8: Residual Risk — Assess remaining risk after treatment. Obtain management acceptance.

3. Likelihood Scale

Score	Rating	Description
1	Rare	May occur only in exceptional circumstances (less than once every 5 years)
2	Unlikely	Could occur but not expected (once every 2-5 years)
3	Possible	Might occur at some time (once every 1-2 years)
4	Likely	Will probably occur in most circumstances (once or more per year)
5	Almost Certain	Expected to occur frequently (multiple times per year)

4. Impact Scale

Score	Rating	Description
1	Negligible	Minimal impact on operations, no regulatory implications, no financial loss
2	Minor	Minor operational disruption, limited financial impact, no regulatory breach
3	Moderate	Noticeable disruption, moderate financial loss, potential regulatory attention
4	Major	Significant disruption, major financial loss, regulatory investigation, reputational damage

© 2026 Nuvencia. All rights reserved.

5	Severe	Business-threatening impact, critical system failure, major regulatory penalties, severe reputational harm

5. Risk Matrix

[Guidance: Risk Score = Likelihood x Impact. Green (1-4) = Low, Yellow (5-9) = Medium, Orange (10-15) = High, Red (16-25) = Critical]

6. Risk Register Format

Use the following columns for your risk register (maintained as a spreadsheet):

Column	Description
Risk ID	Unique identifier (e.g., R-001)
Risk Description	Clear description of the risk scenario
Asset / Process	The asset or process affected
Threat	The threat source or event
Vulnerability	The weakness being exploited
Existing Controls	Current controls in place
Likelihood (1-5)	Probability rating
Impact (1-5)	Impact rating
Risk Score	Likelihood x Impact
Risk Level	Low / Medium / High / Critical
Treatment Option	Mitigate / Transfer / Accept / Avoid
Treatment Plan	Specific actions to treat the risk
Risk Owner	Person accountable for managing the risk
Target Date	Deadline for treatment completion
Residual Risk	Remaining risk score after treatment
Status	Open / In Progress / Closed / Accepted

© 2026 Nuvencia. All rights reserved.