POLICY

Risk Management Procedure

How to identify, score, treat and accept information security risks

Document owner	[Owner name and role]
Approved by	[Approver name and role]
Version	[1.0]
Effective date	[Date]
Next review	[Date, at least yearly]
Classification	[Internal]

Purpose

This procedure sets how [Company Name] identifies, analyzes, evaluates, treats and monitors information security risks, so that assessments are repeatable and results are comparable over time.

This kit includes a risk register spreadsheet and a Statement of Applicability spreadsheet that follow this procedure. Use them as the working records.

Scope

This procedure applies to all information, systems, processes, people and suppliers within the ISMS scope defined in the [ISMS Scope Statement]. It covers risks to the confidentiality, integrity and availability of information.

Roles and responsibilities

Role	Responsibilities
[Security Lead]	Owns this procedure. Runs risk assessments. Maintains the risk register and the Statement of Applicability. Reports risks to top management.
Risk owners	Managers with the authority to decide on a risk. Approve the treatment plan, track actions and accept residual risk within their limit.

Role	Responsibilities
Asset owners	Keep their assets in the inventory, set classification and help identify threats and vulnerabilities.
[Security Committee]	Reviews the risk register at least [quarterly] and challenges scores and treatment progress.
Top management	Approves the risk acceptance criteria and accepts residual risks above the acceptance level.

Procedure

1. Asset inventory

1. The [IT Manager] and asset owners must maintain an inventory of information assets in [asset inventory tool / compliance platform / spreadsheet].
2. The inventory must include at least: asset name, type, owner, classification, location or hosting provider and whether it holds customer or personal data.
3. Asset types include:
    - Information: customer data, source code, financial records, employee records.
    - Software and services: production application, SaaS tools, cloud accounts.
    - Infrastructure: cloud workloads, databases, networks, CI/CD pipelines.
    - Devices: laptops and mobile devices managed by the [MDM].
    - People and suppliers: key roles and critical vendors.
4. The inventory must be reviewed at least every [6 months] and updated when assets are added or removed. Similar assets with the same controls may be grouped, for example "all company laptops".

2. Risk identification

5. For each asset or asset group, identify threats (what could happen) and vulnerabilities (the weakness that allows it). Example: threat "attacker logs in with a stolen password", vulnerability "MFA not enforced on the admin console".
6. Inputs for identification must include: previous incidents, audit findings, vulnerability scan results, supplier assessments, changes to the business and input from asset owners.
7. Each risk must be written as one clear sentence: the cause, the event and the impact.
8. Each risk must have a named risk owner.

3. Risk analysis

9. Risk owners and the [Security Lead] must rate each risk for likelihood and impact on a 1 to 5 scale, using the tables below, considering the controls already in place.

Likelihood scale

Score	Level	Description
1	Rare	Not expected in the next [3] years. No known cases in similar companies.
2	Unlikely	Could happen once in [2 to 3] years.
3	Possible	Could happen once in the next [12 months].
4	Likely	Expected to happen several times a year.
5	Almost certain	Happening now or expected monthly.

Impact scale

Score	Level	Financial	Customers and data	Operations	Legal and reputation
1	Negligible	Less than [amount]	No customer data affected	Downtime under [1 hour]	No external visibility
2	Minor	[amount] to [amount]	Internal data of low sensitivity exposed	Downtime up to [4 hours]	Complaint from one customer
3	Moderate	[amount] to [amount]	Limited confidential data of a few customers	Downtime up to [1 business day]	Contract breach with one customer
4	Major	[amount] to [amount]	Confidential data of many customers	Downtime up to [3 days]	Regulator notification, loss of key customers
5	Severe	More than [amount]	Large personal data breach	Downtime over [3 days]	Fines, legal action, national press

10. When the impact areas give different scores, use the highest one.

4. Risk scoring and evaluation

11. Risk score equals likelihood multiplied by impact, giving a value from 1 to 25.
12. Risks are rated using these bands:

Score	Rating	Required action
1 to 4	Low	Accept and monitor at the next review

Score	Rating	Required action
5 to 9	Medium	Treat when practical, or the risk owner may accept
10 to 15	High	Treatment plan required within [30] days. Only top management may accept.
16 to 25	Critical	Immediate treatment. Escalate to top management within [5] business days.

5. Risk acceptance criteria

13. The acceptance level for [Company Name] is a residual score of [9] or lower. Adjust it to your risk appetite and record top management approval of the chosen value.
14. Risk owners may accept residual risks at or below the acceptance level.
15. Residual risks above the acceptance level must be accepted in writing by [top management], with a reason and a review date no later than [12 months].
16. Acceptance decisions must be recorded in the risk register with name, date and reason.

6. Risk treatment

17. For every risk above the acceptance level, the risk owner must choose one or more treatment options:

- **Modify (mitigate):** add or improve controls to reduce likelihood or impact, for example enforce MFA, enable encryption, add monitoring.
- **Avoid:** stop the activity that causes the risk, for example retire an unsupported system.
- **Share (transfer):** move part of the risk to another party, for example through cyber insurance or a managed service, while staying accountable.
- **Retain (accept):** accept the risk according to the acceptance criteria.

18. Each treatment must have an owner, actions, a due date and the expected residual score.
19. Controls selected for treatment must be compared with Annex A to make sure no needed control has been missed.
20. Treatment actions must be tracked in [ticketing tool] and linked from the risk register.
21. After treatment, the residual risk must be scored again using the same scales.

7. Risk register fields

22. The risk register must contain at least these fields:

Field	Description
Risk ID	Unique reference, for example R-001
Date identified	When the risk was added

Field	Description
Asset or asset group	What is at risk
Threat	What could happen
Vulnerability	The weakness that allows it
Risk description	Cause, event and impact in one sentence
Risk owner	Person accountable for the decision
Existing controls	Controls already in place
Likelihood, Impact, Inherent score	Scores before new treatment
Treatment option	Modify, avoid, share or retain
Treatment actions and due date	What will be done and when, with ticket links
Annex A controls	Related control numbers, for example 5.15, 8.5
Residual likelihood, impact and score	Scores after treatment
Acceptance	Accepted by, date and reason
Status	Open, in treatment, accepted or closed
Next review date	When the risk will be reviewed again

8. Statement of Applicability

23. The [Security Lead] must maintain a Statement of Applicability (SoA), the list of all Annex A controls with the decision for each.
24. For each control the SoA must state: whether it is included or excluded, the reason (for example a risk in the register, a legal or contractual requirement, or a business need), its implementation status and a reference to the policy or evidence.
25. Exclusions must have a clear reason, for example "7.4 Physical security monitoring is excluded because [Company Name] has no office and all infrastructure is hosted by [cloud provider]".
26. The SoA must be updated after every risk assessment and approved by [top management / Security Committee].

9. Review frequency

27. A full risk assessment must take place at least once every [12 months].
28. Additional assessments must take place after significant changes, such as a new product, a new cloud provider, a merger, a major incident or a new legal requirement.

29. The [Security Committee] must review High and Critical risks and treatment progress at least [quarterly], and results must be presented at the management review.
30. Risk owners must update the status of their treatment actions at least [monthly] until closed.

Exceptions

Deviations from this procedure, such as a different scale for one assessment, must be approved by the [Security Lead] and recorded with the reason.

Enforcement

Late treatment actions are reported to the [Security Committee] and, if they persist, to top management. Compliance is checked during internal audits.

Related documents

- Information Security Policy
- Risk register and Statement of Applicability (spreadsheets included in this kit)
- [ISMS Scope Statement] and [Asset inventory]

Annex A mapping

Annex A control	Section that covers it
5.7 Threat intelligence	Risk identification (statement 6)
5.9 Inventory of information and other associated assets	Asset inventory
5.12 Classification of information	Asset inventory (statement 2)
5.31 Legal, statutory, regulatory and contractual requirements	Statement of Applicability, Review frequency
5.35 Independent review of information security	Review frequency
8.8 Management of technical vulnerabilities	Risk identification (statement 6)

Review and approval

The [Security Lead] must review this procedure at least once every [12 months] and when the risk appetite or business changes. Top management approves each version and the acceptance criteria. Changes are shared with all risk owners.