Risk Management Policy

Information Security

Version 1.0

Prepared By:
Hrushikesh Mehendale

Reviewed By:
Shruti Deshpande

FlaggGRC

Document Control

Last Modified	Reason For Change	Suggested By	Approved By
6 April 2025	Document created	Hrushi M	Shruti D
25 Mar 2026	Document reviewed, no change	Hrushi M	Shruti D
7 Oct 2026	Document reviewed, no change	Hrushi M	Shruti D

Purpose

The purpose of the Risk Management Policy shall be to identify, assess, mitigate, and monitor risks to protect the organization’s information assets and ensure business continuity.

Scope

All the staff and third-party users.

Principle

Risks to information security are proactively identified, assessed, and mitigated based on their potential impact and the company appetite. Risk management shall be an ongoing process, integrated into all business activities to enhance security and resilience.

Risk Management Methodology

📓 Risk Register

Risk Identification

Risk identification shall be carried out by:

- Analyzing the organization's context, internal and external issues, and the needs and expectations of interested parties.
- All relevant factors shall be considered to ensure that potential risks to information security are systematically recognized and documented.
- Risks emerging from the practical challenges of implementing the Annex A controls shall also be added to the risk register.

Risk Impact

Risk impact levels shall be assigned to each risk according to the following classification:

- **Level 1 (Negligible Impact):** Minimal or no effect on operations, security, or performance.
- **Level 2 (Task-Specific Impact):** Affects specific tasks or activities without disrupting overall department functions.
- **Level 3 (Department-Wide Impact):** Impacts an entire department but does not extend beyond it.
- **Level 4 (Customer-Wide Impact):** Affects multiple customers or external stakeholders, leading to potential service disruptions or reputational risks.
- **Level 5 (Organization-Wide Impact):** Has a significant effect on the entire organization, potentially leading to major operational, financial, or security consequences.

Risk Likelihood

Risk likelihood levels shall be assigned to each risk based on the following classification:

- **Level 1:** Risks that shall occur once in five years.
- **Level 2:** Risks that shall occur once in a year.
- **Level 3:** Risks that shall occur once in six months.

HaggGRC

- **Level 4:** Risks that shall occur once a month or a quarter.
- **Level 5:** Risks that shall occur once a week.

Risk Score

A risk score shall be calculated and assigned to each identified risk to help assess its importance. The risk score shall be determined using the following formula:

Risk Score = Risk Impact Level × Risk Likelihood Level

This score shall help decide how to handle the risk. Higher scores shall mean the risk needs urgent attention, while lower scores shall indicate less impact on the organization.

Risk Appetite

The company shall have a **moderate risk appetite**, accepting risks with moderate impact and likelihood. Any higher risks shall need extra controls, mitigation, or management approval. All risk decisions shall align with the company's risk management framework and business goals.

Only in exceptional circumstances shall the risks falling in high risk categories shall be accepted.

Acceptable Risk

Acceptable risk score shall define the level of risk the company is willing to accept without requiring additional controls. It shall be calculated as follows:

Acceptable Risk Score = Moderate Risk Impact × Moderate Risk Likelihood

= 2 × 2

= 4

Any risk with a score of 4 or lower shall be considered acceptable, while risks exceeding this threshold shall require treatment measures.

Risk Classification & Mitigation

Each risk shall be classified according to the risk score and the mitigation strategy shall be decided.

Classification	Risk Score	Mitigation Strategy
Minor	1 - 4	Accept risk

FlaggGRC

Moderate	5 - 9	Reduce risk / Accept if reduction not possible
High	10 - 15	Reduce risk / Exceptional acceptance
Severe	16 or above	Reduce risk

Risk Treatment

Once a risk is assessed, the company shall decide how to handle it based on its impact and likelihood. The following treatment options shall be considered:

- **Risk Acceptance**
  - If the risk score is within the acceptable risk threshold, the company shall acknowledge the risk and take no further action beyond routine monitoring.
  - The decision to accept risk shall be approved by the CISO.
  - Here are some key points about risk acceptance:
    - Defined Criteria – The company shall accept risks that fall within its defined risk appetite and acceptable risk score.
    - Informed Decision-Making – Risks shall only be accepted after assessing their impact, likelihood, and potential consequences.
    - Business Justification – Risk acceptance shall be based on cost-benefit analysis, ensuring that mitigation efforts are not disproportionately expensive or impractical.
    - Approval Process – Any accepted risks shall be formally documented and approved by senior management or the designated risk owners.
    - Ongoing Monitoring – Accepted risks shall be continuously monitored to ensure they remain within acceptable levels and do not escalate.
    - Periodic Review – The organization shall regularly review accepted risks to determine if conditions have changed, requiring re-evaluation or mitigation.
    - This approach shall be taken when:
      - It is not cost effective to treat the risk
      - A business of commercial opportunity exists that far outweighs the threat and impact
- **Risk Mitigation**
  - If the risk is too high, the company shall take steps to reduce either its impact or likelihood.
  - This may include implementing stronger security controls, improving processes, training employees, or using technology to lower the risk.
  - The risk mitigation approaches shall be approved by the CISO.
  - Here are some key points about risk mitigation:
    - Reducing Impact or Likelihood – Risk mitigation shall involve taking actions to reduce the impact or likelihood of a risk occurring.

FlagGRC

        - Implementation of Controls – The organization shall apply security controls, policies, and best practices to minimize risk exposure.
        - Proactive Approach – Risk mitigation shall focus on preventing risks before they materialize rather than responding after an incident occurs.
        - Technical and Administrative Measures – Mitigation strategies shall include security technologies, process improvements, training, and access restrictions.
        - Cost-Benefit Analysis – The feasibility of mitigation efforts shall be assessed based on cost, effectiveness, and business needs.
        - Continuous Improvement – Mitigation measures shall be reviewed regularly to ensure they remain effective against evolving risks.
        - Integration with Business Processes – Risk mitigation shall be embedded into daily operations, project management, and decision-making.
        - Monitoring and Reporting – The effectiveness of risk mitigation efforts shall be tracked, documented, and reported to management for ongoing improvements.
- **Risk Transfer**
    - Some risks shall be transferred to third parties through insurance, outsourcing, or contracts.
    - Here are some key points about risk transfer:
        - Shifting Responsibility – Risk transfer shall involve shifting the financial or operational burden of a risk to a third party, such as an insurer or vendor.
        - Insurance Coverage – The company shall obtain appropriate insurance policies (e.g., cyber liability insurance) to cover potential losses from security incidents.
        - Third-Party Contracts – Vendor agreements shall include clauses that ensure suppliers take responsibility for specific risks, such as data breaches or service disruptions.
        - Outsourcing Risks – When outsourcing critical functions, the company shall ensure that service providers comply with security and compliance requirements.
        - Liability Clauses – Contracts with clients, vendors, and partners shall define liability limits and responsibilities in case of security incidents or failures.
        - Indemnification Agreements – The company shall include indemnification clauses in agreements to protect against financial losses due to third-party failures.
        - Risk vs. Cost Consideration – Risk transfer shall be evaluated based on cost-effectiveness and the ability of the third party to manage the risk efficiently.For example, cybersecurity insurance may cover financial losses from a cyberattack, or a vendor may take responsibility for certain security measures.
- **Risk Avoidance**

HaggGRC

- If a risk is too severe and cannot be reduced or transferred, the company shall modify or stop the activity that introduces the risk.
- Some key risk avoidance strategies shall be as follows:
  - Eliminating Risk Sources – The company shall avoid activities, processes, or technologies that introduce unacceptable risks.
  - Secure Design – Systems, policies, and workflows shall be designed in a way that minimizes or eliminates risks from the start.
  - Strict Access Controls – High-risk actions, such as unrestricted administrative access, shall be avoided through role-based access and least privilege principles.
  - Non-Essential Activities – Any function or process that presents significant security risks and is not critical to operations shall be discontinued.
  - Technology Choices – The company shall avoid using outdated or untrusted software and hardware that could expose vulnerabilities.
  - Regulatory Compliance – Any actions that may lead to legal or compliance violations shall be avoided to prevent penalties and reputational damage.
  - Vendor Selection – Vendors with weak security practices shall be avoided to minimize risks from third-party relationships.
  - Cost vs. Benefit Analysis – Risk avoidance shall be implemented where the cost of mitigating or transferring the risk is higher than eliminating the risk altogether.

Review

The organization shall conduct risk management activities at least once annually to identify, assess, and address potential risks. This process shall include reviewing internal and external threats, evaluating the effectiveness of existing controls, and updating risk treatment plans as needed. The risk management process shall be documented, and findings shall be presented to management for review and necessary action.

📓 Reviews Register

Monitoring

The organization shall conduct regular audits of all risk management activities to ensure they are effectively implemented and followed. Monitoring shall verify that risks are identified, assessed, and treated as per the risk management process. Any gaps or issues found shall be documented and addressed by management.

📓 Audits Register

FlaggGRC

Compliance Measurement

The management and CISO shall ensure compliance to this policy by setting the right tone from the top, appropriate provisioning of resources, comprehensive training programs and periodic monitoring activities.

Policy Compliance

Exceptions

Any exception to this policy shall be approved and recorded by the CISO in advance and reported to the Management Review Team.

Non-Compliance

Any staff found to have violated this policy may be subjected to disciplinary action, up to and including termination of employment.

Continual Improvement

This policy is updated and reviewed as part of the continual improvement process.

FlaggGRC