# Risk Management Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives and legal requirements.*

### Security boundary under scope

1. [List of applicable systems]

### References

1. NIST SP 800-30: <https://csrc.nist.gov/pubs/sp/800/30/r1/final>
2. NIST 800-39: <https://csrc.nist.gov/pubs/sp/800/39/final>
3. ISO/IEC 31000: <https://www.iso.org/standard/65694.html>
4. ISO/IEC 27005: <https://www.iso.org/standard/80585.html>
5. ISO/IEC TS 27008: <https://www.iso.org/standard/67397.html>
6. NIST SP 800-115: <https://csrc.nist.gov/pubs/sp/800/115/final>
7. ISO/IEC 27001:2022: 4.1, 5.1.g, 6.1.1.a, 6.1.1.b, 6.1.1.c, 6.1.1.e, 6.1.2, 6.1.3, 8.1.a, 8.1.b, 8.2, 8.3, 9.1, 9.2.1, 9.3, 10.1, 10.2.d
8. NIST 800-53 rev. 5: CA-2, CA-2(1), CA-2(3), CA-5, CA-7(1), CA-7(4), RA-1, RA-2, RA-3, RA-7, SI-2(3), SI-6, SR-1
9. CIS v8: 7.2, 7.7
10. PCI DSS 4.0: 1.2.7, 2.2.5, 5.2.3.1, 12.3.1, 12.3.2
11. AICPA SOC 2 TSC: CC1.2, CC3.1, CC3.2, CC3.3, CC3.4, CC4.1, CC5.1, CC5.2, CC9.1

## Document ownership

 <(Choose from)>

* 1. Policy Owner:
		1. [Owner name] ([Owner email]), [Owner title]
	2. Information Security Officer:
		1. [Information officer name], ([Information officer email]), [Information officer title]
	3. System Owner(s):
		1. [System owner name], ([System owner email]), [System owner title]
	4. Process and Operational Owner(s)
		1. [process owner], ([process owner email]), [process owner title]
	5. System Administrator(s):
		1. [System admin name], ([System admin email]), [System admin title]
	6. Required Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT
	7. Optional Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT

## Purpose

The purpose of this Risk Management Policy is to establish a comprehensive and structured approach to identifying, assessing, managing, and mitigating risks that could potentially impact the organization’s ability to achieve its objectives. This policy aims to ensure that risks are effectively managed across all levels of the organization, enhancing decision-making, safeguarding assets, and maintaining operational resilience. By implementing this policy, the organization commits to proactively addressing risks to protect its assets, reputation, and stakeholders.

## Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals or entities engaged with the organization. It encompasses all aspects of the organization's operations, including but not limited to:

* Information Technology and Cybersecurity
* Operational Processes
* Financial Management
* Legal and Regulatory Compliance
* Human Resources
* Physical Security
* Third-Party and Supply Chain Management

The policy covers the entire risk management lifecycle, including risk identification, assessment, treatment, monitoring, and reporting. It ensures that all risks are systematically managed in alignment with the organization's strategic objectives and regulatory requirements. This policy is mandatory for all relevant parties and must be adhered to in conjunction with other related policies and procedures within the organization.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], [owner title] | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | Executive Team | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | Executive Team | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], [Information officer title] | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner], Operational owner title] |  |
| Information Systems Administrators | System Administrators  | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], [HR title] | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users |  End Users | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | [provider type] | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
	2. Management has reviewed and approved this policy.
	3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
	4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
	2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. Risk Management System: A coordinated set of activities and methods used to direct an organization and control the many risks that can affect its ability to achieve objectives.
	2. Risk Register: A documented record of identified risks, including their status, assessment, and treatment plans. It serves as a central repository for all risk-related information.
	3. Risk Assessment: The process of identifying, analyzing, and evaluating risks to determine their potential impact and likelihood, using industry-standard methodologies.
	4. Risk Treatment: The process of selecting and implementing measures to modify risk, including risk transfer, mitigation, acceptance, or avoidance.
	5. Risk Transfer: A risk treatment option where the risk is shifted to another party, typically through insurance or outsourcing.
	6. Risk Mitigation: A risk treatment option that involves taking steps to reduce the likelihood or impact of a risk.
	7. Risk Acceptance: A risk treatment option where no action is taken to alter the risk, but it is acknowledged and monitored.
	8. Risk Avoidance: A risk treatment option where actions are taken to eliminate the risk entirely, often by discontinuing the activities that generate the risk.
	9. Management Review: A systematic evaluation conducted by the organization’s leadership to ensure the risk management process is effective and aligned with the organization’s objectives.
	10. Third-Party Risk Management: The process of assessing and managing risks associated with vendors, suppliers, and other external entities that can affect the organization’s security posture.
	11. Supply Chain Risk Management: The process of identifying and managing risks related to the supply chain to ensure the integrity and security of the organization’s operations and products.
	12. Security Controls: Safeguards or countermeasures put in place to reduce the risk to an organization's assets, including physical, technical, and administrative controls.
	13. Deficiencies: Identified weaknesses or gaps in the risk management process or the effectiveness of controls that need to be addressed.
	14. Corrective Action Plans: Plans developed to address deficiencies, including steps to improve processes or controls to mitigate identified risks.

## Policy

#### Risk Management System

The [responsible party] shall:

* + 1. Establish a risk management system that includes a comprehensive risk register to document identified risks, their assessment, and treatment plans.
		2. Ensure that the risk register is maintained and updated regularly to reflect new and emerging risks, as well as the status of existing risks.
		3. Utilize the risk register to track the progress of risk treatment plans and document risk owners responsible for each risk.

#### Leadership and the Board

The [responsible party] shall:

* + 1. Report identified business risks and their status to the organization's leadership and the board at least quarterly, or more frequently if significant risks are identified.
		2. Provide risk assessment reports that include the potential impact, likelihood, and recommended mitigation strategies for each risk.
		3. Ensure that critical risks are communicated promptly to the leadership and the board to facilitate timely decision-making.

#### Risk Assessments

The [responsible party] shall:

* + 1. Conduct risk assessments at least annually, or when significant changes occur, using industry-standard methodologies such as NIST SP 800-30 and ISO/IEC 27005.
		2. Identify threats, vulnerabilities, and potential impacts to the organization's assets, processes, and operations.
		3. Conduct regular assessments of the effectiveness of security controls to ensure they adequately mitigate identified risks.
		4. Document the findings of the risk assessments in a formal report, including a risk action plan for mitigating or managing identified risks.

#### Risk Treatment

The [responsible party] shall:

* + 1. Evaluate and decide on appropriate risk treatment options, including risk transfer, mitigation, acceptance, or avoidance.
		2. Develop and implement risk treatment plans for each identified risk, prioritizing actions based on the severity and likelihood of the risks.
		3. Monitor the effectiveness of risk treatment plans and update them as necessary to address any changes in the risk landscape or organizational environment​​​​.

#### Management Review

The [responsible party] shall:

* + 1. Conduct regular reviews of the risk management process and the effectiveness of risk treatment plans.
		2. Ensure that risk management activities are aligned with the organization's strategic objectives and regulatory requirements.
		3. Update the risk management process and associated documentation based on the outcomes of management reviews and changes in the risk environment.

#### Third-party and Supply Chain Risk Management

The [responsible party] shall:

* + 1. Establish a third-party risk management program to assess and manage risks associated with vendors, suppliers, and other third parties.
		2. Conduct regular risk assessments of third-party vendors and supply chain partners, considering their impact on the organization's security posture.
		3. Require third-party vendors to adhere to the organization's security requirements and to report any security incidents or vulnerabilities that may affect the organization​​.

#### Corrective Action Plans

The [responsible party] shall:

* + 1. Track identified deficiencies in the risk management process and the effectiveness of controls.
		2. Document deficiencies and assign responsibility for addressing each deficiency.
		3. Develop corrective action plans to address identified deficiencies and improve the organization's risk management process.
		4. Ensure that corrective actions are implemented within agreed timelines and that their effectiveness is monitored.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
	2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
	3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
		1. Policies
		2. Procedures
		3. Standards
		4. Documentation
		5. Regulations
		6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
	2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
		1. The Information Security Officer
		2. Officer of the [Organization name] Leadership Team
	3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |