INFORMATION SECURITY RISK MANAGEMENT FRAMEWORK

1. Document Control

DOCUMENT CONTROL	
Document ID	*[Enter Document Reference Number]*
Version	*[e.g., 1.0]*
Status	*[Draft / Under Review / Approved]*
Classification	*[e.g., Internal Use Only]*
Document Owner	*[Title of Responsible Role/Function]*
Approved By	*[Title of Approving Authority]*
Date	*[DD/MM/YYYY]*
Applicable Standard	*ISO/IEC 27001:2022 — Clauses 6.1.1 (General), 6.1.2 (Risk Assessment), 6.1.3 (Risk Treatment), 8.2, 8.3 | Cross-ref: 4.1, 4.2, 4.3, 6.2, 9.1*

2. Revision History

Version	Date	Author / Role	Description of Change
1.0	*[DD Month YYYY]*	*[ISMS Manager / Risk Lead]*	Initial draft
[e.g., 1.1]	*[DD Month YYYY]*	*[Role / Name]*	*[Description of change]*
[e.g., 1.1]	*[DD Month YYYY]*	*[Role / Name]*	*[Description of change]*
[e.g., 1.1]	*[DD Month YYYY]*	*[Role / Name]*	*[Description of change]*

3. Introduction

A process approach and risk-based thinking are essential for identifying organizational needs and creating an effective Information Security Management System (ISMS). This approach is crucial for developing, implementing, and improving these systems to enhance customer satisfaction by meeting requirements. It involves the systematic definition and management of processes and their interactions to achieve intended results aligned with the organization's quality policy, Information security policy and strategic direction.

Risk-based thinking, integral to an effective ISMS by addresses potential non-conformity through preventive actions and analysis. To establish a comprehensive risk management framework, ISO 31000 is referenced as a standard.

4. Risk Management Objectives

[Organization Name] shall establish and maintain a Risk Management Framework to systematically identify, assess, treat, and monitor risks that may impact the achievement of its strategic, operational, regulatory, and information security objectives.

Risk management shall support informed decision-making and ensure alignment with the organization's business goals, regulatory obligations, customer commitments, and long-term sustainability.

The Organization shall ensure that risk management activities protect the confidentiality, integrity, and availability (CIA) of information assets within the defined ISMS scope and that appropriate controls are implemented based on risk severity and business criticality.

[Organization Name] is committed to the continual improvement of its Risk Management Framework through periodic reviews, management oversight, monitoring of emerging risks, lessons learned from incidents, and alignment with applicable legal, regulatory, and industry standards.

> **Fill-in criteria:** *Align this section with the organization's mission, regulatory environment, and strategic priorities. Define the review authority (e.g., Top Management / Risk Committee) and confirm how CIA protection aligns with applicable regulatory requirements and internal data classification policies.*

5. Scope

This Risk Management Framework applies to all information assets, systems, applications, infrastructure components, business processes, personnel, third-party services, and physical locations that fall within the formally approved Information Security Management System (ISMS) scope.

The scope of risk management shall be fully aligned with the approved ISMS Scope Document and shall cover all activities, products, and services that could impact the confidentiality, integrity, and availability (CIA) of information assets within that boundary.

Risk assessments shall be conducted considering:

- The organization's internal and external context
- Business objectives and strategic direction
- Legal, statutory, regulatory, and contractual obligations
- Requirements of interested parties
- Interfaces, integrations, and dependencies with external organizations, service providers, and supply chain partners

For each asset, system, or process within scope, risks shall be identified, analyzed, and evaluated against threats that may compromise confidentiality, integrity, and availability.

> **Fill-in criteria:** *Confirm that the scope described here matches the approved ISMS Scope Document. If any systems, sites, or activities are excluded from risk assessment, list them clearly and provide a brief reason. Ensure that confidentiality, integrity, and availability are assessed for all in-scope assets.*

6. Risk Appetite and Tolerance

[Organization Name] shall define and maintain a formal Risk Appetite and Risk Tolerance Statement to establish the level and type of risk the Organization is willing to accept in pursuit of its strategic, operational, and regulatory objectives.

Risk Appetite represents the overall amount of risk that [Organization Name] is prepared to accept in achieving its business goals, while Risk Tolerance defines the acceptable variation or deviation from established risk thresholds.

6.1 Risk Appetite

The Organization shall accept risks only where:

- The assessed risk value falls within the defined Risk Acceptance Criteria.
- The risk does not result in violation of applicable legal, statutory, regulatory, or contractual obligations.
- The risk does not materially impact customer trust, brand reputation, or business continuity.
- The residual risk, after treatment, remains within approved tolerance limits.

Risks exceeding defined appetite thresholds require mandatory treatment, avoidance, transfer, or formal escalation.

> **Fill-in criteria:** *Define the specific numerical and/or qualitative thresholds that represent acceptable risk (e.g., Risk Value ≤ 10 or "Medium and below"). Ensure the stated appetite aligns with board-approved strategy, regulatory obligations, and business continuity requirements.*

6.2 Zero-Tolerance Areas

[Organization Name] shall maintain zero tolerance for risks that may result in:

- Regulatory or statutory non-compliance.
- Unauthorized disclosure of sensitive, personal, or confidential information.
- Intentional violation of security policies or ethical standards.
- Fraud, corruption, or unlawful activities.

- Significant compromise of safety, critical infrastructure, or essential service availability.

Such risks shall not be accepted and shall require immediate mitigation or avoidance actions, with mandatory escalation to Top Management.

> **Fill-in criteria:** *Clearly specify organization-specific zero-tolerance categories based on industry, regulatory environment, and contractual commitments (e.g., RBI non-compliance, personal data breach, financial fraud). Ensure these areas are formally endorsed by Top Management.*

6.3 Risk Tolerance and Escalation Thresholds

The Organization shall define quantitative and/or qualitative thresholds that determine when a risk must be escalated.

At a minimum:

- Risks categorized as High or Very High shall be escalated to Senior Management.
- Risks exceeding defined acceptance criteria shall not be closed without documented management approval.
- Residual risks above tolerance levels shall trigger additional treatment or formal risk acceptance at an appropriate authority level.

Escalation decisions shall be documented in the Risk Register and reviewed during Management Review meetings.

> **Fill-in criteria:** *Define quantitative escalation triggers (e.g., Risk Value ≥ 16 requires Executive approval) and document the approval hierarchy. Confirm how and where escalation decisions are recorded (e.g., Risk Register, Management Review minutes).*

The Risk Appetite and Tolerance Statement shall be reviewed at least annually or upon significant organizational, regulatory, or strategic change to ensure continued relevance and alignment with business objectives.

7. Determining the internal and external issues

The Organization shall systematically determine, document, and periodically review the internal and external issues that are relevant to its purpose, strategic direction, and operational context, and that may affect its ability to achieve the intended results of the Information Security Management System (ISMS).

The Head of Department or Project Manager shall be responsible for identifying and defining department-specific internal and external issues that may influence business objectives, regulatory compliance, service delivery, information security posture, and overall risk exposure.

Internal issues may include, but are not limited to:

- Organizational structure, governance, and decision-making processes
- Roles, responsibilities, and competency levels
- Corporate culture and risk appetite
- Policies, procedures, and control effectiveness
- Technology infrastructure and system dependencies
- Financial resources and operational capabilities
- Historical incidents, audit findings, and performance trends

External issues may include, but are not limited to:

- Applicable legal, statutory, and regulatory requirements
- Industry standards, contractual obligations, and certification commitments
- Market conditions and competitive landscape
- Technological advancements and evolving threat environment
- Economic, political, and environmental factors
- Third-party, supplier, and outsourcing dependencies
- Customer expectations and stakeholder requirements

Identified internal and external issues shall be documented in the Context Register or equivalent documented information and shall be subjected to risk assessment in accordance with the Organization's Risk Management Methodology.

8. Risk Process

[Organization Name] shall implement a structured and repeatable Risk Management Process aligned with ISO 31000, ISO/IEC 27005, and NIST SP 800-30 principles. The process ensures systematic identification, categorization, analysis, and evaluation of risks that may impact business objectives, service delivery, and the confidentiality, integrity, and availability of information assets.

The Risk Process consists of the following stages:

- Risk Identification
- Risk Categorization

- Risk Assessment
- Risk Value
- Risk Acceptance criteria
- Risk Treatment Options
- Post Risk Treatment and Residual Risk
- Risk Ownership

8.1 Risk Identification

The purpose of Risk Identification is to determine events, conditions, or circumstances that may cause potential loss, disruption, non-compliance, or compromise of information assets. The objective is to understand how, where, and why such risks may occur.

Risk identification shall be conducted:

- During project initiation and planning phases
- During onboarding of new systems, services, or locations
- Upon significant organizational or regulatory change
- During periodic risk review cycles
- Following major incidents or audit findings

Risk sources may include threats, vulnerabilities, process weaknesses, human factors, system failures, third-party dependencies, and environmental conditions.

Identified risks shall be documented in the Risk Register (Document ID) with clear risk descriptions, affected assets, and potential impact areas.

8.2 Risk Categorization

For consistency and structured analysis, identified risks shall be categorized under one of the following domains:

- **Process** – Risks related to core and supporting business processes delivering customer services.
- **Technology** – Risks arising from IT systems, applications, infrastructure, tools, and technical platforms.
- **People** – Risks associated with employees, contractors, third parties, and other interested parties.
- **Location** – Facility-related risks including physical security, environmental threats, and site dependencies.

- **Miscellaneous** – Risks not falling under the above categories but impacting organizational objectives.

Categorization supports risk trend analysis, reporting, and prioritization.

8.3 Risk Assessment

[Organization Name] has adopted a combined qualitative and quantitative approach for Risk Assessment.

Risk Assessment shall evaluate:

1. Likelihood (Probability of Occurrence)
2. Impact (Consequence on Business and Information Security)
3. Effect on Confidentiality, Integrity, and Availability (CIA)

The initial step of the assessment shall determine whether the risk results in potential Loss of Confidentiality (C), Integrity (I), or Availability (A), or a combination thereof.

8.3.1 Likelihood Scale

Likelihood represents the probability or frequency of occurrence of a risk event.

Rating	Level	Description
1	Rare	Highly unlikely to occur, if ever
2	Unlikely	May occur once in approximately three years
3	Possible	May occur once annually
4	Likely	Expected to occur multiple times per year
5	Almost Certain	Expected to occur monthly or more frequently

The likelihood rating scale ranges from 1 (Lowest) to 5 (Highest).

8.3.2 Impact Scale

Impact represents the severity of consequences on service delivery, operational efficiency, and business objectives.

Rating	Level	Service Delivery Interruption	Operational Impact
1	Insignificant	Less than 1 hour	Minimal disruption
2	Negligible	1 to 8.5 hours	Minor inconvenience
3	Moderate	1 day to 1 week	Delays in major deliverables
4	Major	1 week to 1 month	Failure of major deliverable
5	Extreme	More than 1 month	Failure of key corporate objectives

Impact rating scale ranges from 1 (Lowest) to 5 (Highest).

8.4 Risk Value Determination

The Risk Value shall be calculated by the Head of Department or Project Manager using the defined likelihood (probability) and impact ratings.

Risk Value = Probability × Impact

Impact \ Likelihood	L1: Rare	L2: Unlikely	L3: Possible	L4: Likely	L5: Almost Certain
Impact: 5 Extreme	5 Very Low	10 Low	15 Medium	**20 High**	**25 Very High**
Impact: 4 Major	4 Very Low	8 Low	12 Medium	**16 High**	**20 High**
Impact: 3 Moderate	3 Very Low	6 Low	9 Low	12 Medium	15 Medium
Impact: 2 Negligible	2 Very Low	4 very Low	6 Low	8 Low	10 Low
Impact: 1 Insignificant	1 Very Low	2 Very Low	3 Very Low	4 Very Low	5 Very Low

The risk rating ranges from **1 to 25**, based on a 5×5 matrix model.

Risk Value	Risk Exposure Level
1 – 5	Very Low
6 – 10	Low
11 – 15	Medium
16 – 20	**High**
21 – 25	**Very High**

The calculated score represents the **inherent risk value** prior to treatment. Risk exposure levels shall guide prioritization, escalation, and treatment decisions.

8.5 Risk Acceptance Criteria

The Organization shall define risk acceptance thresholds consistent with its risk appetite and operational tolerance.

Unless otherwise justified, all identified risks shall be treated where mitigation is feasible and does not impose disproportionate cost or operational constraints.

Risk may be accepted under the following conditions:

1. Where the Risk Value is **≤ 10 (Low or Very Low exposure)**.
2. Where a documented exception is formally reviewed and approved by Management.
3. Where the cost of treatment exceeds the potential impact, and acceptance is risk-informed and justified.

All accepted risks shall be:

- Documented in the Risk Register
- Approved by authorized Management
- Periodically reviewed for continued validity

8.6 Risk Treatment Options

[Organization Name] shall implement risk treatment in accordance with its approved Risk Assessment Methodology and Risk Appetite Statement. Risk treatment shall aim to reduce risk exposure to an acceptable level while ensuring compliance with applicable legal, regulatory, and contractual obligations.

Risk treatment decisions shall be formally documented in the Risk Register and implemented.

> **Fill-in criteria:** *Specify the document ID number used for Risk Register.*

8.6.1 Risk Acceptance

Risk Acceptance involves formally acknowledging a risk and continuing operations without implementing additional controls, provided the risk remains within defined tolerance levels.

Risk may be accepted where:

- The risk value falls within the approved risk appetite threshold.
- The cost of mitigation exceeds the potential business impact.
- No feasible control is available.
- The exposure is temporary and monitored.

> **Fill-in criteria:** *Define the numerical threshold for acceptance (e.g., Risk Value ≤ 10). Specify who has authority to approve accepted risks and define the validity period of acceptance (e.g., 6 months / 1 year).*
>
> *All accepted risks shall be documented with business justification and management approval.*
>
> *Confirm where acceptance evidence will be maintained (e.g., Risk Register column, approval email, management meeting minutes).*

8.6.2 Risk Avoidance

[Organization Name] implement risk avoidance by eliminating activities, systems, processes, or engagements that give rise to unacceptable risk exposure where such risks exceed the defined risk tolerance and cannot be effectively mitigated, transferred, or otherwise controlled.

8.6.3 Risk Mitigation (Risk Reduction)

[Organization Name] shall implement risk mitigation by establishing and applying appropriate administrative, technical, physical, and contractual controls to reduce the likelihood and/or impact of identified risks to an acceptable level in alignment with its approved risk appetite and applicable regulatory, contractual, and standards requirements.

All mitigation actions shall be formally documented in the risk register and shall include clearly defined control measures, assigned control owners, defined implementation timelines, and mandatory reassessment of residual risk following control implementation. Control selection shall align with the Organization’s internal control framework and, where applicable, be mapped to relevant standards such as ISO/IEC 27001 and reflected in the Statement of Applicability.

> **Fill-in criteria:** *If needed define the maximum allowed timeframe for treatment implementation (e.g., High risks within 30 days). Ensure residual risk calculation is mandatory post-implementation.*

8.6.4 Risk Transfer

[Organization Name] shall implement risk transfer by formally shifting part or all of the identified risk exposure to a qualified third party through contractual agreements, insurance coverage, or outsourcing arrangements, where such transfer is consistent with the approved risk appetite and business objectives.

All risk transfer arrangements shall be formally documented in the Risk Register and Risk Treatment Plan and shall include defined contractual safeguards, assigned oversight responsibility, defined monitoring mechanisms, and periodic reassessment of residual risk. Prior to transferring risk, [Organization Name] shall conduct appropriate due diligence and third-party risk assessment to ensure that security, compliance, service-level, liability, and audit requirements are clearly established in legally binding agreements. Residual risk remaining after transfer shall be evaluated against the defined risk acceptance criteria and approved by authorized management

8.6.5 Risk Treatment Selection Criteria

[Organization Name] shall ensure that the selection of an appropriate risk treatment strategy is based on a structured and risk-informed decision-making process aligned with its Risk Appetite and strategic objectives. In determining the most suitable treatment option, the Organization shall consider, at a minimum:

- Applicable legal, statutory, and regulatory requirements.
- Contractual commitments and customer obligations.
- Alignment with business objectives and strategic priorities.
- Cost-benefit and proportionality analysis of proposed controls.
- Impact on operational efficiency and service continuity.
- The level of residual risk remaining after treatment implementation.

Risk treatment decisions shall be proportionate to the level of risk exposure and shall not compromise regulatory compliance or critical business operations. Where treatment decisions may materially impact compliance posture, financial performance, or strategic direction, escalation to Top Management shall be mandatory.

All treatment decisions shall be formally documented in the Risk Register and Risk Treatment Plan, including justification for the selected approach, and shall remain traceable for audit and review purposes. Treatment effectiveness shall be periodically reviewed to ensure continued adequacy and alignment with the Organization’s risk environment.

8.7 Post-Treatment and Residual Risk Management

Upon completion of risk treatment activities, [Organization Name] shall reassess the treated risks to determine the effectiveness of implemented controls and to calculate the revised (residual) risk value.

Where applicable, ISO/IEC 27001 controls and other relevant internal or regulatory controls shall be applied to reduce the level of risk in alignment with the approved Risk Treatment Plan and Statement of Applicability.

The revised risk value (Residual Risk) shall:

- Be recalculated using the approved risk assessment methodology.
- Be equal to or lower than the inherent risk value prior to treatment.
- Be evaluated against the defined Risk Acceptance Criteria.

If the residual risk remains above the approved acceptance threshold, the risk shall be:

- Escalated to authorized Management for review.
- Subject to additional treatment measures; or
- Formally accepted with documented justification and management approval.

No risk shall be considered closed until residual risk has been formally evaluated, documented in the Risk Register, and approved by the designated authority.

8.8 Risk Ownership

Each department head of [Organization Name] shall assign a designated Risk Owner for each identified risk to ensure clear accountability, authority, and oversight throughout the risk management lifecycle. The Risk Owner shall be a role or individual directly associated with the relevant business process, system, or operational function and shall possess sufficient authority to influence decisions and allocate resources necessary for effective risk management.

All identified risks shall have a formally documented Risk Owner recorded in the Risk Register. The Risk Owner shall be responsible for validating the risk assessment, selecting and approving appropriate treatment actions, ensuring timely implementation of control measures, monitoring treatment effectiveness, and escalating risks that exceed defined acceptance criteria to the appropriate management level. Risk ownership remain active until the risk is formally treated, accepted, or closed in accordance with this framework.

9. Risk Register

[Organization Name] shall establish, implement, and maintain a Risk Register as controlled documented information to record, track, and monitor all identified risks within the approved scope of the Risk Management Framework.

Each risk entry shall clearly articulate the threat scenario, including the source of risk, potential vulnerability, and the business or operational impact on confidentiality, integrity, availability, service delivery, regulatory compliance, or strategic objectives.

The Risk Register shall be version-controlled and maintained in accordance with the Documented Information Procedure to ensure integrity, traceability, and audit readiness. Access to the Risk Register shall be restricted to authorized personnel to maintain confidentiality and prevent unauthorized modification.

The approved Risk Register Template (Document ID: [Insert Document ID]) shall be used consistently across all departments to document:

- Internal and external issues
- Needs and expectations of interested parties
- Risk Process

No risk shall be considered formally identified, treated, accepted, or closed unless recorded in the approved Risk Register template.

10. Roles and Responsibilities

[Organization Name] shall define and maintain clear roles, responsibilities, and authorities to ensure effective implementation, oversight, and continual improvement of the Risk Management Framework. Roles shall be documented, communicated, and supported by adequate resources to ensure accountability at all organizational levels.

10.1 Top Management

Top Management shall provide leadership and strategic direction for risk management and shall:

- Approve the Risk Management Framework and Risk Appetite Statement.
- Ensure risk management is integrated into business processes and strategic planning.
- Allocate adequate resources for risk treatment and monitoring.
- Review significant risks, residual risks, and risk treatment effectiveness.
- Approve high-risk acceptance and zero-tolerance exceptions (if applicable).

Top Management shall demonstrate commitment to risk governance through periodic Management Review meetings.

> **Fill-in criteria:** *Specify the governing body responsible (e.g., Board of Directors, Executive Committee) and define review frequency (e.g., quarterly or annually).*

10.2 Risk Management Function / ISMS Manager / CISO

The designated Risk Management authority shall:

- Develop, implement, and maintain the Risk Management Framework.
- Facilitate risk assessments across departments.
- Ensure consistency in risk evaluation and scoring methodology.
- Maintain the centralized Risk Register.
- Monitor compliance with risk treatment plans.
- Report significant risks to Top Management.

This function shall ensure alignment with ISO/IEC 27001, regulatory requirements, and internal governance standards.

> **Fill-in criteria:** *Define the official role title (e.g., CISO, ISMS Manager, Risk Manager) and reporting line within the organization.*

10.3 Department Heads

Each Department Head shall:

- Ensure identification of risks within their functional area.
- Assign Risk Owners for identified risks.
- Approve risk treatment actions within delegated authority.

- Escalate risks exceeding defined tolerance thresholds.
- Ensure implementation of agreed mitigation controls.

Department Heads are accountable for managing risks within their operational domain.

Fill-in criteria: *Clarify authority limits for departmental risk acceptance (e.g., up to Medium risks only).*

10.4 Risk Owners

Risk Owners shall be responsible for the day-to-day management of assigned risks and shall:

- Validate risk assessment details.
- Implement and monitor risk treatment actions.
- Ensure timely reassessment of residual risk.
- Report changes in risk status.
- Escalate unresolved or elevated risks.

Risk Owners shall maintain accountability until the risk is formally closed or accepted.

Fill-in criteria: *Define eligible designations for Risk Owners and ensure formal documentation in the Risk Register.*

10.5 Employees and Interested Parties

All employees, contractors, and relevant third parties shall:

- Comply with the Risk Management Framework and associated policies.
- Identify and report new or emerging risks.
- Support implementation of mitigation controls within their responsibilities.

Risk awareness shall form part of organizational training and communication programs.

Fill-in criteria: *Specify reporting channels for risk identification (e.g., email, GRC tool, incident portal).*

11. Monitoring and Reporting

[Organization Name] shall establish and maintain a structured Risk Monitoring and Review process to ensure that identified risks remain within defined tolerance levels and that the Risk Management Framework continues to operate effectively, efficiently, and in alignment with organizational objectives and regulatory requirements.

11.1 Review Frequency

All identified risks shall be reviewed at [defined intervals] to confirm the continued accuracy of risk assessments, effectiveness of implemented controls, and validity of residual risk levels. High and Very High risks shall be reviewed [more frequently], while Medium and Low risks shall be reviewed at least [annually]. The overall Risk Management Framework shall undergo a formal review at least [once per year] by [Risk management Team], as part of the Management Review process to ensure its ongoing suitability, adequacy, and effectiveness.

> **Fill-in criteria:** *Specify the exact review frequency for each risk category and confirm who is responsible for conducting and approving periodic review.*

11.2 Trigger-Based Reviews

In addition to scheduled reviews, risk reassessment shall be initiated whenever significant internal or external events occur that may alter the organization’s risk profile. Such events include security incidents, audit findings, major organizational or technological changes, introduction of new services or systems, regulatory updates, or material changes in the threat landscape. Following such trigger events, the relevant risks shall be reassessed and the Risk Register updated within a defined and reasonable timeframe.

> **Fill-in criteria:** *Define the maximum timeframe within which reassessment must be completed after a trigger event and specify the responsible role for initiating the review.*

11.3 Management Reporting

All identified risks, including their assessment results, treatment status, residual risk levels, and escalation requirements, shall be formally reported to Management at defined intervals.

Risk reporting shall include, at a minimum:

- Summary of High and Very High risks.
- Risks exceeding defined tolerance or appetite thresholds.
- Status of risk treatment plans and overdue actions.
- Residual risks pending approval.
- Emerging or newly identified significant risks.

Risk reports shall support risk-based decision-making and resource allocation and shall be documented as part of governance records.

> **Fill-in criteria:** *Specify the reporting format (e.g., dashboard, formal report), reporting frequency, and the designated recipients such as Executive Management, Risk Committee, or Board.*

12. Policy Review and Approval

This Risk Management Framework shall be reviewed at least annually, or upon significant organizational, regulatory, or operational change, to ensure its continued suitability, adequacy, and effectiveness.

The policy shall be approved by Top Management and shall be communicated to relevant stakeholders to ensure awareness and compliance.

> **Fill-in criteria:** *Specify review frequency (e.g., annually), approval authority (e.g., CEO, Board of Directors), and document control reference number.*

— End of Document —

This document is provided as a generic template. All sections, context references, and fill-in guidance fields must be reviewed and customized to reflect the Organization's specific business environment, regulatory requirements, and governance structure prior to formal approval and adoption.