RISK ASSESSMENT METHODOLOGY

INLINE WITH ISO 27001:2022 & SOC 2 TYPE 2

PREPARED BY

MINISTRY OF MOS SECURITY

Document Name	**Risk Assessment Methodology**
Classification	**Internal Use Only**

Document Management Information

Document Title:	Risk Assessment Methodology
Document Number:	ORGANISATION-RISK-ASM-MTD
Document Classification:	Internal Use Only
Document Status:	Approved

Issue Details

Release Date	DD-MM-YYYY

Revision Details

Version No.	**Revision Date**	**Particulars**	**Approved by**
1.0	DD-MM-YYYY	<Provide details of changes made on policy here>	<Provide name of Approver here>

Document Contact Details

Role	**Name**	**Designation**
Author	<Provide name of author here>	<Provide designation of author here>
Reviewer/ Custodian	<Provide name of reviewer here>	<Provide designation of reviewer here>
Owner	<Provide name of owner here>	<Provide designation of owner here>

Distribution List

Name
Need Based Circulation Only

CONTENTS

1. PURPOSE

The purpose of this methodology is to establish a standardized, repeatable, and auditable process for identifying, assessing, treating, and monitoring information security risks associated with enterprise assets across [ORG NAME].

This methodology ensures that:

- Risks to the **confidentiality**, **integrity**, and **availability** (CIA) of information assets are systematically evaluated and prioritized based on their impact and likelihood.
- Risk treatment decisions are **aligned with the organization's risk appetite**, legal/regulatory requirements, and **ISO/IEC 27001:2022 Clause 6.1.2.**
- Risk management activities are performed in accordance with the principles outlined in **ISO/IEC 27005:2022** and **ISO 31000:2018**, supporting informed decision-making and continual improvement of the Information Security Management System (ISMS).
- Asset-based risk visibility is improved to support **resource allocation**, **incident prevention**, **compliance assurance**, and **resilience planning**.

2. SCOPE

This risk assessment methodology applies to all information assets owned, controlled, processed, or accessed by [ORG NAME], regardless of format, location, or medium.

It covers:

- **Physical assets** such as servers, workstations, laptops, mobile devices, and storage media
- **Logical assets** such as software, applications, databases, credentials, source code, and intellectual property
- **Information assets,** including structured and unstructured data, reports, documentation, and communications
- **Human assets** including employees, contractors, third-party users, and administrators
- **Technological infrastructure** including cloud services, virtual environments, and networking systems
- **Third-party and outsourced services** that process or store [ORG NAME] data or integrate with its systems

This methodology is applicable across all organizational functions, departments, and geographies and must be used for:

- Initial and periodic risk assessments
- Asset onboarding or classification changes
- Significant changes to IT infrastructure, processes, or business operations
- Pre and post-implementation of major projects or technologies
- Security incident root cause analysis and risk re-evaluation

3. TERMS AND DEFINITIONS

Term	Definition
Asset	Any item of value to the organization, including physical devices, software, data, infrastructure, or personnel.
Risk	The potential for loss or harm to an asset arising from a threat exploiting a vulnerability.
Risk Owner	The individual or entity responsible for managing and accepting the outcome of a specific risk.
Threat	A potential cause of an unwanted incident that may result in harm to a system or organization.
Vulnerability	A weakness in an asset, system, or process that can be exploited by a threat.
Impact	The magnitude of harm that could be caused if a threat exploits a vulnerability.
Likelihood	The probability or frequency that a specific threat will successfully exploit a vulnerability.
Inherent Risk	The level of risk present before any control or mitigation measures are applied.

Residual Risk	The remaining risk after implementing mitigation controls or treatments.
Risk Appetite	The amount and type of risk an organization is willing to accept in pursuit of its objectives.
Risk Tolerance	The acceptable variation in outcomes related to specific risks.
Risk Treatment	The process of selecting and implementing measures to modify risk (e.g., avoid, mitigate, transfer, accept).
Control	A measure that is implemented to reduce risk by preventing or detecting threats or vulnerabilities.
Risk Assessment	The process of identifying, analyzing, and evaluating risk to inform decision-making.
Risk Evaluation	The process of comparing risk levels against pre-defined criteria to determine their significance or priority.
Information Asset	Data or information that has value to the organization and requires protection.

4. ROLES AND RESPONSIBILITIES

Role	**Responsibilities**
Chief Information Security Officer (CISO)	- Owns the overall risk methodology - Approves high/critical risk acceptance - Escalates to executive management - Reviews exception requests and residual risk justifications
Information Security Officer (ISO)	- Facilitates risk assessments and scoring validation - Reviews control selection and treatment plans - Approves medium-risk exceptions - Oversees risk register maintenance and audit readiness

Role	**Responsibilities**
Risk Owner	- Identifies, reviews, and owns assigned risks - Selects appropriate treatment options - Ensures timely implementation - Submits risk acceptance requests and updates
Risk Assessor / Analyst	- Conducts risk identification, scoring, and documentation - Calculates residual risk and control strength - Updates risk register and assessment reports
Asset Owner	- Identifies and classifies assets - Provides input on asset valuation and impact - Participates in threat relevance review
Control Owner	- Implements selected controls as per treatment plans - Reports progress and effectiveness - Supports control strength evaluation
Department Head / Process Owner	- Reviews and validates risk relevance to business processes - Approves risk treatment timelines and resource commitments - Escalates unresolved issues to ISO/CISO
Information Security Team	- Maintains risk register and exception register - Monitors risk trends and compliance gaps - Prepares dashboards and audit documentation - Coordinates residual risk and incident response reviews
Risk Committee / Exec Management	- Reviews critical risk scenarios - Makes risk-informed decisions aligned with business priorities - Oversees governance, risk appetite, and strategic alignment
Internal Audit / Compliance Team	- Validates risk documentation accuracy - Tests control effectiveness and adherence to methodology - Flags non-compliance or recurring gaps

5. RISK MANAGEMENT PRINCIPLES

The risk assessment methodology at [ORG NAME] is based on the core principles of risk management as defined in ISO 31000:2018 and extended through ISO/IEC 27005:2022 for application to information security. These principles ensure that risk management is effective, structured, and aligned with the organization's strategic goals.

Principle	Description
Integrated	Risk management is embedded in all business and security processes across the organization.
Structured and Comprehensive	A consistent, repeatable process ensures reliable and comparable risk assessments.
Customized	The methodology is tailored to [ORG NAME]'s context, including its risk appetite, regulatory environment, and business objectives.
Inclusive	Risk identification and analysis involve relevant stakeholders to leverage operational and technical expertise.
Dynamic	The methodology is flexible and responsive to change, adapting to evolving threat landscapes and organizational priorities.
Uses Best Available Information	Risk decisions are based on accurate, relevant, and up-to-date data from both internal and external sources.
Human and Cultural Factors	Recognizes that human behavior, awareness, and culture influence information security risks.
Continual Improvement	The methodology is regularly reviewed and improved based on feedback, incidents, audits, and performance metrics.

These principles provide a foundation for consistent and defensible risk-based decision-making, enabling [ORG NAME] to manage information security risks effectively and strategically.

6. RISK ASSESSMENT PROCESS

6.1. ASSET IDENTIFICATION AND VALUATION

Purpose

To establish a structured process for identifying, recording, and valuing all organizational assets that may be impacted by information security risks.

1. Asset Identification

- All information assets, including physical, logical, and informational elements, must be recorded in the centralized **Asset Inventory Register**, managed under the Asset Management Policy.
- Each asset must be uniquely identified and linked to:
  - **Asset Owner**
  - **Location**
  - **Associated business process or system**
  - **Confidentiality, Integrity, Availability (CIA) attributes**
- Assets include (but are not limited to):
  - Hardware (servers, laptops, networking devices)
  - Software (applications, licenses, codebases)
  - Information (data sets, customer records, documents)
  - People (roles with privileged access)
  - Services (third-party providers, cloud platforms)
  - Infrastructure (data centers, physical facilities)

2. Asset Valuation

- Assets are assigned a value based on their importance to the organization's objectives and the potential impact on the **CIA triad**.
- Valuation is conducted using a **qualitative scale** (Low, Medium, High) with criteria such as:
  - Business impact if the asset is lost, altered, or unavailable
  - Number of customers or stakeholders affected

- Financial loss or downtime implications
- Legal or regulatory consequences
- Reputational damage

3. Asset Valuation Reference Table (Scored for Risk Calculation)

Criterion	Low (1)	Medium (2)	High (3)
Confidentiality	Public or non-sensitive data	Internal/moderately sensitive information	Confidential, regulated, or sensitive information (e.g., PII, IP)
Integrity	Minor impact if modified; non-critical data	Operational inconvenience or service degradation	Critical process failure or data alteration affects decision-making
Availability	Temporary disruption is acceptable	Moderate disruption; recoverable downtime	Business-critical systems; SLA-bound or real-time dependency
Customers Affected	None or very few (<10)	Dozens to hundreds (10–500)	Hundreds to thousands (>500); external-facing
Financial Impact	<$1,000	$1,000 – $50,000	>$50,000 or recurring financial loss
Legal/Regulatory Impact	No legal/regulatory implications	Contractual or moderate compliance exposure	Breach of major laws/regulations; fines or sanctions
Reputation Damage	No public or internal impact	Internal dissatisfaction or limited third-party concern	Media exposure, customer trust loss, or public stakeholder impact

Each asset is assigned a **single value** reflecting its overall importance to [ORG NAME], based on its sensitivity, business dependency, and risk exposure.

Asset Value	Classification	Description
1	Low Value Asset	Limited impact on confidentiality, integrity, or availability. Loss or misuse would not disrupt operations or cause financial, legal, or reputational harm.
2	Medium Value Asset	Moderate impact on business operations or internal processes. Asset may support essential functions or contain internal-only data.
3	High Value Asset	Critical to business continuity or compliance. May store or process sensitive, regulated, or customer-impacting information. Loss or compromise would result in severe disruption or penalty.

6.2. THREAT IDENTIFICATION

1. Purpose

To systematically identify potential threats that could exploit vulnerabilities and compromise the confidentiality, integrity, or availability of organizational assets.

2. Threat Definition

A **threat** is any circumstance or event—intentional or accidental—that has the potential to adversely impact an asset by exploiting its vulnerabilities.

Threats can originate from internal or external sources and may be natural, technical, environmental, or human in nature.

3. Threat Categories

Category	Examples
Human (Intentional)	Insider threats, social engineering, sabotage, phishing, hacking
Human (Unintentional)	Human error, misconfiguration, accidental deletion, negligence
Technical	Malware, ransomware, software bugs, system crashes, zero-day exploits
Environmental	Fire, flood, power failure, hardware overheating, HVAC failure
Physical	Theft, unauthorized access, vandalism, loss of devices

Category	**Examples**
Third-Party	Vendor compromise, service provider failure, cloud misconfigurations

4. Threat Identification Process

Asset-based Mapping: For each asset, identify applicable threat categories using:

- Historical incidents
- Threat intelligence feeds
- Industry databases (e.g., OWASP, MITRE ATT&CK, ENISA threat landscape)
- Input from Asset Owners and System Administrators

Threat Relevance Assessment:

- Evaluate whether each threat is **plausible** and **relevant** based on:
  - Exposure level of the asset (internal vs. external)
  - Known threat actors or trends
  - Environmental or operational context

Documentation:

- List all applicable threats per asset in the **Risk Register** with:
  - Threat description
  - Source (internal/external)
  - Classification (intentional/unintentional)
  - Supporting rationale

6.3. VULNERABILITY ASSESSMENT

1. Purpose

To identify and evaluate vulnerabilities—technical, procedural, or organizational—that may be exploited by identified threats, increasing the likelihood of asset compromise.

2. Vulnerability Definition

A **vulnerability** is a weakness or gap in an asset, system, or control that could be exploited by a threat to cause harm to the organization.

Vulnerabilities can exist in software, hardware, processes, configurations, or even in human behaviour.

3. Vulnerability Categories

Category	Examples
Technical	Unpatched systems, misconfigured firewalls, weak authentication mechanisms
Process / Policy	Lack of documented procedures, poor access control implementation
People / Human	Lack of awareness, phishing susceptibility, untrained staff
Physical / Environmental	Unlocked server rooms, exposed cables, inadequate fire suppression systems
Third-Party	Insufficient due diligence on vendors, reliance on unverified external APIs

4. Vulnerability Scoring

Each vulnerability is evaluated on a **qualitative scale** for its **severity and exploitability**:

Vulnerability Level	Score	Description
Low	1	Difficult to exploit or mitigated by strong controls
Medium	2	Possible to exploit under certain conditions; controls exist but may be weak
High	3	Easily exploitable; controls are absent or ineffective

5. Sources of Vulnerability Identification

- Internal and external vulnerability scans
- Penetration test results
- Security audit findings
- Incident postmortems
- Configuration reviews
- Vendor security advisories

6.4. IMPACT ASSESSMENT

1. Purpose

To evaluate the potential consequences of a successful threat exploiting a vulnerability on the organization's operations, finances, reputation, legal obligations, and overall security posture.

2. Definition of Impact

Impact is the **degree of damage or loss** that would occur if an identified risk materializes. Impact is considered across multiple business dimensions, including:

- Confidentiality breach (e.g., data leakage)
- Integrity compromise (e.g., unauthorized changes)
- Availability loss (e.g., system downtime)

- Financial loss
- Legal or regulatory exposure
- Reputational damage

- Operational disruption

3. Impact Scoring Scale

Use a **qualitative scale** mapped to **numerical values** for consistency in risk scoring:

Impact Level	Score	Description
Low	1	Minor inconvenience or degradation; no regulatory or financial loss
Medium	2	Noticeable disruption; localized financial or compliance impact
High	3	Severe disruption to operations, legal penalties, or significant reputational harm

Impact Assessment Reference Table (Scored 1–3)

Impact Dimension	Low (1)	Medium (2)	High (3)
Financial Loss	<$1,000	$1,000 – $50,000	>$50,000 or recurring losses
Legal / Regulatory	No legal/regulatory exposure	Minor contractual or compliance exposure	Major law/regulatory breach; fines or litigation risk
Reputation	No brand or stakeholder impact	Internal concern or limited stakeholder visibility	Public/media exposure; loss of customer or investor trust
Operational Disruption	Minimal effect on non-critical functions	Temporary disruption to departmental services	Major outage of critical systems/processes

Data Sensitivity	Public or low-sensitivity information	Confidential internal information	Regulated, personal, or highly sensitive data (e.g., PII, IP, credentials)
Number of Systems Affected	Single system or low-dependency device	Affected systems support one or two departments	Multiple interconnected or enterprise-wide systems were impacted
Number of Customers Affected	None or <10	10–500 (internal or external)	>500 customers; public-facing or mission-critical customer groups

4. Usage Guidelines

- During assessment, evaluate **each applicable dimension**.
- The **highest applicable score** across any of the 7 dimensions becomes the **Impact Score (1–3)**.
- This ensures that even a single severe consequence (e.g., public data breach or critical system outage) results in a “High Impact” risk classification.

6.5. LIKELIHOOD ASSESSMENT

1. Purpose

To estimate the **probability or frequency** of a threat exploiting a vulnerability and successfully impacting an asset, forming a key component of risk scoring.

2. Definition of Likelihood

Likelihood refers to the **chance** that a specific threat scenario will occur, based on known threat behaviors, vulnerability exposure, and existing control effectiveness.

Likelihood Scoring Scale (with Frequency)

Likelihood Level	Score	Frequency / Timeframe	Description
Low	1	**Unlikely (Once in a year)**	The event is rare; no known occurrences internally or in similar environments; strong controls exist.
Medium	2	**Possible (Once every Month)**	An event has occurred in similar environments or internally on rare occasions; some controls are in place.
High	3	**Likely (At least once per week)**	The event has occurred previously; controls are weak, or the asset is highly exposed.

3. Likelihood Evaluation Criteria

When assessing likelihood, consider:

Factor	Examples
Threat Capability	Sophistication, resources, or motivation of attackers
Control Maturity	Control effectiveness (preventive, detective, corrective)
Asset Exposure	Accessibility (public-facing, cloud-based, third-party integrated)
Historical Incidents	Internal or industry-specific breach trends
Environmental Factors	Location-specific threats (e.g., power, flood), political or regional risks

4. Sources for Likelihood Estimation

- Internal incident history and logs
- Threat intelligence feeds and advisories
- Audit and vulnerability scan results
- MITRE ATT&CK or ENISA threat landscape reports
- Control testing outcomes

Threat Score = Threat Impact (1–3) × Likelihood (1–3)

This gives a possible **Threat Score range from 1 to 9**.

Threat Score Interpretation Table

Threat Impact (x-axis) ↓ / Likelihood (y-axis) →	Low (1)	Medium (2)	High (3)
Low (1)	1	2	3
Medium (2)	2	4	6
High (3)	3	6	9

6.6. RISK EVALUATION AND RISK MATRIX

1. Purpose

To evaluate the significance of identified risks by calculating a composite score based on asset value, threat likelihood and impact, and vulnerability. This step determines the priority of treatment and required level of management attention.

2. Risk Score Calculation Formula

Each risk is scored using the following formula:

Risk Score = Asset Value× Threat Score ×Vulnerability Score

- **Asset Value**: Represents the importance and sensitivity of the asset (Low = 1, Medium = 2, High = 3)

- **Threat Score = Threat Impact × Likelihood**:
    - Threat Impact (1–3)×Likelihood (1–3)=1 to 9
    - Determines the potential impact score (range: 1–9)
- **Vulnerability Score**: Represents the ease with which the asset can be compromised (Low = 1, Medium = 2, High = 3)

3. Risk Score Range

- Minimum Risk Score: 1
- Maximum Risk Score: 81

4. Risk Rating and Prioritization

Risk Score Range	Risk Level	Treatment Priority
1 – 10	Low	Acceptable; monitor periodically; document risk acceptance
11 – 30	Medium	Treat with standard controls; schedule risk owner review
31 – 60	High	Prompt treatment required; escalate to department head or ISO
61 – 81	Critical	Immediate action required; escalate to CISO and Risk Committee

7. RISK APPETITE AND RISK ACCEPTANCE CRITERIA

7.1. RISK APPETITE

1. Definition

Risk Appetite is the amount and type of risk that [ORG NAME] is **willing to accept** in pursuit of its strategic and operational objectives. It provides boundaries for decision-making, investment in controls, and risk treatment prioritization.

2. Risk Appetite Statement

[ORG NAME] maintains a **low to moderate risk appetite** for information security risks, especially those that may impact:

- Personally Identifiable Information (PII)
- Regulated or contractual data (e.g., HIPAA, GDPR, PCI-DSS)

- Core business operations and availability
- Reputational standing with customers and partners

High or critical risks that threaten the above areas are considered **unacceptable** and must be **treated or escalated without delay**.

7.2. RISK ACCEPTANCE CRITERIA

1. Definition

Risk Acceptance refers to the **formal acknowledgment and approval** to retain a risk without further treatment, based on its assessed severity and alignment with the organization's risk appetite.

2. Acceptance Thresholds

Risk Level	Risk Score Range	Acceptance Criteria	Approving Authority
Low	1 – 10	Acceptable by default; monitor periodically	Risk Owner
Medium	11 – 30	Acceptable with justification; documented monitoring plan	Department Head + Information Security
High	31 – 60	Acceptance only with strong justification and compensating controls	CISO + Risk Committee (case-by-case)
Critical	61 – 81	Not acceptable unless supported by business-critical exemption & escalation	CISO + CEO / Executive Management

3. Risk Acceptance Process

1. Risk Assessor calculates and categorizes the risk.
2. Risk Owner submits a **Risk Acceptance Form** with justification (business rationale, cost-benefit, compensating controls).
3. The Information Security Team validates the documentation.
4. Final approval is granted based on the authority matrix.
5. All accepted risks are:
   - Recorded in the **Risk Register**
   - Assigned a **review date** (typically within 3 to 6 months)

  - Subject to reassessment upon any significant change

8. RISK TREATMENT

1. Purpose

To define how [ORG NAME] selects, implements, and monitors appropriate actions to modify identified information security risks in accordance with its risk appetite and strategic objectives.

2. Risk Treatment Options

In alignment with ISO/IEC 27005:2022, four treatment strategies are available:

Treatment Option	Description	Examples
Avoid the Risk	Discontinue the activity that causes the risk.	Cancel risky projects or decommission a vulnerable system.
Mitigate the Risk	Implement controls to reduce the likelihood or impact of the risk.	Deploy firewalls, patch systems, conduct awareness training.
Transfer the Risk	Shift risk exposure to a third party.	Purchase cyber insurance, outsource to managed service providers.
Accept the Risk	Formally acknowledge and retain the risk without additional controls, within risk acceptance limits.	Document acceptance and monitor regularly.

---

3. Control Selection and Implementation

- Controls must be selected from:
  - **ISO/IEC 27001:2022 Annex A** (or equivalent control frameworks like NIST CSF, CIS)
  - Existing organizational standards and policies
- Factors for control selection:
  - Risk severity and score
  - Control effectiveness and feasibility
  - Legal and regulatory obligations

    - Cost-benefit considerations

Each control must be:

- Assigned to a responsible **owner**
- Supported with a timeline and measurable outcomes
- Validated for effectiveness after implementation

4. Risk Treatment Plan

Each risk requiring action must be documented in a **Risk Treatment Plan**, including:

- Risk description and score
- Chosen treatment option
- Proposed control(s) or mitigating action(s)
- Owner of the implementation
- Due dates and progress milestones
- Estimated residual risk post-treatment

9. CONTROL STRENGTH AND RESIDUAL RISK

1. Purpose

To assess the effectiveness of existing controls and determine the **residual risk** that remains after controls are applied. This allows informed decision-making on whether a risk is acceptable or requires further treatment.

2. Control Strength Assessment

Control strength is determined by evaluating the **type** and **nature** of the primary control(s) applied to mitigate the risk.

Step 1: Assign Control Strength Score

Assign a **Control Strength Score (1 to 3)** based on two factors:

A. Control Type Score

Type	Score
Preventive	3
Detective	2
Corrective	1

B. Control Nature Score

Nature	Score
Automated & Enforced	3
Semi-Automated / Monitored	2
Manual / Policy-Based	1

Step 2: Calculate Total Control Strength

Control Strength (1 –9) = Control Type Score × Control Nature Score

Step 3: Residual Risk Formula

Residual Risk Score=Control Strength/Risk Score

- **Risk Score** = Asset × Threat Impact × Likelihood × Vulnerability
- **Control Strength** = 1 (weak) to 9 (strong)
- **Residual Risk** output remains comparable to original risk scale (1–81), but accounts for mitigation effectiveness.

🎯 Example

Factor	Value
Asset Value	3
Threat Impact	3
Likelihood	3
Vulnerability	2
Risk Score	3 × (3×3) × 2 = 54
Control Type	Preventive (3)
Control Nature	Automated (3)
Control Strength	3 × 3 = 9
Residual Risk	54 / 9 = 6 → Low

3. Residual Risk Acceptance Table

Residual Risk Score Range	Risk Level	Acceptable?	Action Required
1 – 10	Low	✅ Yes	Acceptable; monitor periodically
11 – 30	Medium	❌ No	Treat using standard controls; assign to Risk Owner
31 – 60	High	❌ No	Escalate to CISO; apply enhanced or layered controls
61 – 81	Critical	❌ No	Immediate action; escalate to Risk Committee or Executives

10. RISK MONITORING AND REVIEW

1. Purpose

To ensure that identified risks, treatment plans, and controls are actively monitored, periodically reviewed, and updated in response to changes in business operations, technology, threat landscape, or compliance requirements.

2. Ongoing Monitoring Activities

Activity	Frequency	Responsible Party
Risk Register Review	Quarterly	Information Security Team
Control Effectiveness Testing	Semi-annually or as defined in treatment plan	Control Owner / Internal Audit
Vulnerability Re-scans	Monthly / Post-change	IT Operations / Security Team
Residual Risk Re-assessment	Aligned with treatment timelines	Risk Owner / Risk Assessor
Security Incident Analysis	Real-time / Post-incident	Incident Response Team
Threat Intelligence Updates	Monthly / As received	Information Security Team

3. Review Triggers

Risk assessments and treatment plans must be **revisited immediately** if any of the following occur:

- Significant changes in asset value, ownership, or usage
- New threats or vulnerabilities are discovered
- Security incidents affecting similar assets or controls
- Changes in legal, regulatory, or contractual obligations
- Implementation of new technologies or infrastructure
- Business process changes (e.g., mergers, expansions, outsourcing)

4. Documentation and Version Control

- All updates to risk scores, controls, treatment status, or ownership must be recorded in the **Risk Register** and must be version-controlled.
- The **Risk Treatment Plan** must reflect:
  - Status updates
  - Residual risk evaluations
  - Closure justifications
- Archived versions must be retained in accordance with the **Data Retention Policy** (minimum 3 years or as required by law).

5. Reporting and Communication

- Risk summaries, outstanding high/critical risks, and treatment status shall be reported:
  - **Quarterly** to the Information Security Committee
  - **Annually** to Executive Management as part of the ISMS Management Review
- Reports may include:
  - Risk heat maps
  - Residual risk trend analysis
  - Top risks dashboard
  - SLA adherence for control implementation

11. RISK REGISTER MAINTENANCE

1. Purpose

To maintain a centralized, accurate, and up-to-date repository of all identified risks, their assessments, treatment plans, and current status for tracking, reporting, and audit purposes.

2. Risk Register Contents

The **Risk Register** must contain the following minimum fields for each risk entry:

Field	Description
Risk ID	Unique identifier
Asset Name	Associated asset or asset group
Asset Value	Assigned criticality (1–3)
Threat Description	Identified threat scenario
Vulnerability	Related weakness or exposure
Threat Impact	Estimated impact (1–3)
Likelihood	Estimated probability (1–3)
Impact Score	Threat Impact × Likelihood (1–9)
Risk Score	Asset Value × Impact Score × Vulnerability Score (1–81)
Control Strength	Control Type × Control Nature (1–9)
Residual Risk Score	Risk Score ÷ Control Strength
Risk Level	Low, Medium, High, Critical (based on residual score)
Treatment Option	Avoid, Mitigate, Transfer, Accept
Treatment Plan / Control Summary	Controls selected or actions taken
Owner	Assigned Risk Owner
Status	Open, In Progress, Closed, Accepted
Next Review Date	Scheduled reassessment date
Last Updated / Version	Timestamp and version of the latest update

3. Risk Register Format

- Maintained in a **secure, centralized system** (e.g., ISMS platform, GRC tool, encrypted spreadsheet).
- Access must be restricted to authorized roles (e.g., Risk Owners, ISO, CISO).

- Versioning and audit trails must be enabled.

4. Review and Update Frequency

Risk Category	Update Frequency
High / Critical	At least **quarterly** or upon change
Medium	At least **semi-annually**
Low	At least **annually**

12. REPORTING AND COMMUNICATION

1. Purpose

To define the mechanisms and frequency for communicating risk-related information to stakeholders, management, and governance bodies, ensuring timely awareness, accountability, and decision-making.

2. Reporting Objectives

- Keep stakeholders informed about risk posture, trends, and treatment status
- Escalate unresolved or critical risks to appropriate decision-makers
- Support strategic planning and resource allocation
- Satisfy internal, regulatory, and audit requirements

3. Reporting Frequency

Audience	Report Type	Frequency
Information Security Committee	Risk dashboard, high-risk updates, treatment progress	Quarterly
Executive Management	Top risks, risk trend analysis, risk appetite alignment	Annually (or as needed)
Risk Owners / Dept. Heads	Assigned risks, overdue treatments, residual risk review	Monthly / Quarterly
Internal Audit / Compliance	Risk register snapshot, residual risk closure reports	On request / Audit cycle
External Stakeholders (if required)	Regulatory risk disclosures, assurance reports	As required (e.g., SOC 2, ISO audits)

4. Reporting Formats

Reports may include:

- Risk Heat Maps (based on residual scores)
- Top N Risks Summary
- Risk Score Distribution Charts
- Treatment Plan Compliance Status
- SLA / Due Date Breaches
- Residual Risk Trends (quarter-over-quarter)

Visuals and summaries should be tailored to the audience (e.g., exec-friendly dashboards vs. technical breakdowns for IT and Security).

5. Communication Channels

- ISMS/GRC platform dashboards
- Email-based reporting (secured and access-controlled)
- Committee meetings or workshops
- Board reports / executive summaries
- Incident management escalations (for emergent risks)

13. DOCUMENTATION AND AUDIT REQUIREMENTS

1. Purpose

To ensure all risk management activities and decisions are properly documented, maintained, and made available for internal review, external audits, and regulatory compliance.

2. Required Documentation

Document	Description
Risk Register	Central record of all identified risks, scores, status, and treatment actions
Risk Assessment Reports	Detailed record of individual or system-wide risk assessments
Risk Treatment Plans	Action plans including controls selected, owners, and implementation timelines

Document	**Description**
Risk Acceptance Forms	Approved exceptions with business justification, review date, and residual risk details
Risk Review Meeting Minutes	Summary of discussions and decisions made during committee or stakeholder meetings
Audit and Control Validation Records	Test results of control implementation and effectiveness
Residual Risk Evaluations	Calculations and rationale behind residual risk categorization
Exceptions Register	List of all accepted or escalated exceptions with approval traceability

3. Record Retention Requirements

Document Type	**Retention Period**	**Justification**
Risk Register	Minimum **3 years**	ISMS audit and accountability
Risk Assessment Reports	Minimum **3 years**	ISO 27001 and internal audit readiness
Acceptance Forms	Minimum **3 years**	Evidence of governance and approvals
Audit Records	Per internal audit policy	Reference for compliance verification

4. Audit Readiness

- All documentation must be:
  - Stored in a **centralized, access-controlled location**
  - Version-controlled and time-stamped
  - Made available to:
    - Internal audit teams
    - External auditors (e.g., ISO 27001, SOC 2 assessors)
    - Regulatory authorities (as required)
- Audit findings related to risk management shall be:
  - Reviewed by the **Information Security Team**

  - Discussed in **quarterly risk committee meetings**
  - Addressed through **corrective and preventive actions (CAPA)**

14. ENFORCEMENT

1. Purpose

To define the consequences of non-compliance with this risk assessment methodology and to ensure accountability for maintaining the integrity of [ORG NAME]'s information security risk management program.

2. Compliance Requirement

- All employees, contractors, consultants, and third-party service providers involved in asset ownership, risk assessment, treatment, or monitoring are **required to comply** with this methodology.
- Compliance will be verified through:
  - Internal audits
  - ISMS reviews
  - Monitoring of treatment plans and risk register entries

3. Examples of Non-Compliance

- Failure to assess risks as per the defined methodology
- Delayed or undocumented treatment of high/critical risks
- Inaccurate or incomplete entries in the Risk Register
- Unauthorized acceptance of non-acceptable residual risks
- Tampering with, or failing to retain, audit trail documentation

4. Disciplinary Actions

Violations may result in corrective or disciplinary action based on the severity, impact, and intent, including:

Severity	**Potential Consequences**
Minor	Verbal or written warning, retraining
Moderate	Temporary access suspension, formal HR warning
Major or Repeat	Revocation of access rights, involvement of HR and Legal teams

Severity	Potential Consequences
Severe or Negligent	Termination of employment/contract, legal action, or escalation to regulators

5. Incident Handling

- All suspected violations must be reported to the **Information Security Team** or **CISO** immediately.
- Each incident will be investigated in line with the **Incident Management Policy**, and appropriate **corrective and preventive actions (CAPA)** will be documented.

15. POLICY EXCEPTIONS

1. Purpose

To define the process for requesting and approving deviations from the defined risk assessment methodology, in cases where full compliance is not feasible due to valid business, technical, or operational reasons.

2. Exception Scenarios

Exceptions may be requested in the following scenarios (not exhaustive):

- Inability to complete a risk assessment by the scheduled due date
- Temporary acceptance of high or critical residual risk due to business urgency
- Deviation from defined scoring or valuation models for legacy or non-standard assets
- Postponement of control implementation beyond defined SLA timelines

3. Exception Request Process

Step	Action
1	Submit a **Policy Exception Request Form** with detailed justification
2	Include risk impact, duration, and any **compensating controls** proposed
3	Exception reviewed by the Information Security Team for risk implications
4	Final approval follows a **multi-tier matrix** (see 16.4 below)

4. Exception Approval Matrix

Level	Approver	Applicable When
Level 1	Department Head	For operational exceptions with minor risk impact
Level 2	Information Security Officer (ISO)	For medium-risk deviations and extended timelines
Level 3	Chief Information Security Officer (CISO)	For exceptions involving high/critical risks, or model deviations

All approved exceptions must be formally documented and tracked.

5. Duration and Review

- **The default validity** of exceptions is **up to 90 days**, unless explicitly extended
- Each active exception must be **reviewed monthly** by the Information Security Team
- Expired exceptions must be closed or revalidated with new approval

6. Exception Register

- All approved exceptions must be recorded in an **Exception Register** with:
  - Exception ID
  - Requester and approvers
  - Duration and expiry date
  - Description and justification
  - Compensating controls (if any)
  - Risk mitigation follow-up actions

7. Auditability and Revocation

- Exceptions are subject to internal and external audit
- The CISO may **revoke** any exception if:
  - The associated risk becomes unacceptable
  - Business justification no longer applies
  - Evidence of misuse, negligence, or non-compliance is found

16. ESCALATION MATRIX

1. Purpose

To ensure that unresolved risks, overdue treatments, or critical compliance gaps are escalated through the appropriate chain of command for timely resolution, accountability, and visibility.

2. Escalation Triggers

Escalation is required in the following scenarios:

- Failure to initiate or complete a risk assessment as scheduled
- Delayed implementation of controls beyond approved timelines
- Acceptance of high or critical risks without formal approval
- Inaccurate or missing risk register entries
- Breach of policy requirements, scoring models, or exception handling
- Detection of emerging high-risk scenarios requiring urgent attention

3. Escalation Matrix

Escalation Level	Role / Designation	Responsibility	Escalation Mode
Level 1	Risk Owner / Control Owner	First-level resolution, clarification of risk status	Email / Ticketing Tool
Level 2	Department Head / Process Owner	Resolve department-level delays or conflicts	Email / Internal Meeting
Level 3	Information Security Officer (ISO)	Validate compliance, treatment effectiveness, and exception risk	Escalation Tool / Phone
Level 4	Chief Information Security Officer (CISO)	Approve or reject risk acceptance, enforce policy governance	Formal Escalation via Email
Level 5	Risk Committee / Executive Sponsor	Resolve enterprise-level or strategic risks	Escalation Memo / Executive Report

4. Documentation Requirements

Each escalation event must be:

- Logged in the ITSM or GRC platform
- Include details such as:
  - Risk ID or reference
  - Date of escalation
  - Description of issue or delay
  - Actions taken and outcomes
- Assigned a tracking ID and reviewed during committee meetings

5. Resolution Timeframes

Escalation levels must be acted upon within the following response timelines:

Level	**Expected Resolution Time**
Level 1	Within 3 business days
Level 2	Within 5 business days
Level 3	Within 5 business days
Level 4	Immediate or <2 business days
Level 5	As per board or committee urgency