# RISK MANAGEMENT POLICY

**of**

# Cosmix LLP

# DOCUMENT INFORMATION

| | |
|---|---|
| **Document:** | RISK MANAGEMENT POLICY |
| **Document Number:** | COS/POL/11 |
| **Version:** | 1.0 |
| **Document Date:** | 17-06-2026 |
| **Prepared By:** | HOD-IT |
| **Reviewed By:** | CISO |
| **Approved By:** | CEO |
| **Classification Level:** | Internal |

**Modification History**

| Sl. No. | Description of Change | Review Date | Version No. |
|---|---|---|---|
| 1 | Initial Basic Release | **17-06-2026** | 1.0 |
| | | | |
| | | | |
| | | | |
| | | | |

# Contents


| Sl. No. | Contents | Page No |
|---|---|---|
| 1 | Purpose | |
| 2 | Scope | |
| 3 | Risk Management Framework | |
| 4 | Roles & Responsibilities | |
| 5 | Risk Assessment & Evaluation | |
| 6 | Risk Treatment | |
| 7 | Risk Register & Residual Risk | |
| 8 | Monitoring, Review & Continuous Improvement | |
| 9 | Documentation, Exceptions & Policy Review | |

## 1. PURPOSE

The purpose of this Policy is to establish a structured framework for identifying, assessing, treating, monitoring, and reviewing information security risks that may impact the confidentiality, integrity, and availability of LLP's information assets. The Policy supports informed decision-making, regulatory compliance, business continuity, and continual improvement of the Information Security Management (ISM).

## 2. SCOPE

- This Policy applies to all information assets, business processes, applications, systems, cloud services, infrastructure, and third-party services within the scope of LLP's ISM.
- The Policy is applicable to all Designated Partners, employees, consultants, contractors, interns, vendors, and third parties who access, process, manage, or store organizational information.

## 3. RISK MANAGEMENT FRAMEWORK

LLP shall implement a continuous risk management process that includes:

- Identification of information security risks;
- Analysis of threats, vulnerabilities, and existing controls;
- Evaluation and prioritization of risks;
- Selection and implementation of appropriate treatment measures;
- Monitoring of residual risks;
- Periodic review of risk treatment effectiveness; and
- Continuous improvement of risk management practices.

Risk assessments shall be performed during implementation of new projects, technologies, business processes, organizational changes, regulatory updates, significant security incidents, onboarding of critical vendors, and at least annually.

## 4. ROLES AND RESPONSIBILITIES

- Top Management/ Founding Member/ CEO shall establish the organization's risk appetite, approve significant risk acceptance decisions, allocate necessary resources, and oversee the effectiveness of the risk management framework.
- Information Security Function shall coordinate risk assessments, maintain the Risk Register, monitor mitigation activities, and report significant risks to management.
- Department Heads and Process Owners shall identify risks within their functional areas, nominate Risk Owners, implement approved controls, and monitor mitigation activities.
- Risk Owners shall evaluate assigned risks, recommend treatment options, implement corrective actions, monitor residual risks, and update the Risk Register.

## 5. RISK ASSESSMENT AND EVALUATION

- Risk assessments shall consider the business impact of identified risks on:
  a) Confidentiality
  b) Integrity
  c) Availability (CIA)
- Each parameter shall be rated as Low (1), Medium (2), or High (3). The combined CIA score shall represent the overall business impact.
- Likelihood shall be assessed using a five-point scale ranging from Rare (1) to Almost Certain (5), considering historical incidents, existing controls, vulnerability exposure, and current threat intelligence.

- The overall Risk Score shall be calculated using:
  **Risk Score = CIA Impact × Likelihood**

  Risk classification shall be:

| Risk Score | Risk Level | Required Action |
|---|---|---|
| 1–9 | Low | Accept and monitor |
| 10–20 | Medium | Mitigate through planned actions |
| 21–35 | High | Priority mitigation |
| 36–45 | Critical | Immediate management action |

## 6. RISK TREATMENT

- Risks exceeding the approved risk tolerance shall be addressed through documented Risk Treatment Plans identifying the Risk Owner, mitigation measures, implementation timeline, and expected residual risk.
- The organization may adopt one or more of the following treatment options:
  a) Reduce the risk through administrative, technical, physical, or contractual controls.
  b) Avoid the activity introducing unacceptable risk.
  c) Transfer the risk through contractual arrangements, outsourcing, or insurance.
  d) Accept the residual risk where it falls within approved organizational tolerance and receives formal management approval.
- As a general guideline, Critical risks shall be addressed immediately, High risks within 30–60 days, Medium risks within 2–4 months, and Low risks during routine improvement activities.

## 7. RISK REGISTER AND RESIDUAL RISK

- All identified risks shall be recorded in a centralized Risk Register containing the risk description, affected asset, threat, vulnerability, existing controls, CIA rating, likelihood, overall risk score, treatment strategy, Risk Owner, mitigation status, review date, and residual risk.
- Upon implementation of mitigation measures, risks shall be reassessed to determine the residual risk. Where residual risks exceed the approved

acceptance level, additional controls or formal management approval shall be obtained.

## 8. MONITORING, REVIEW AND CONTINUOUS IMPROVEMENT

- Risk management shall be monitored continuously through periodic reviews, internal audits, vulnerability assessments, penetration testing, incident analysis, management reviews, and regulatory compliance activities.
- Risk assessments shall be reviewed whenever significant business, technological, legal, or operational changes occur and at least once every year to ensure continued effectiveness of implemented controls.
- Lessons learned from audits, security incidents, emerging threats, and stakeholder feedback shall be incorporated into the continual improvement of the ISM.

## 9. DOCUMENTATION, EXCEPTIONS, AND POLICY REVIEW

- All risk assessment records, treatment plans, management approvals, and supporting evidence shall be securely maintained in accordance with LLP's document retention requirements.
- Any exception to this Policy shall be supported by documented business justification, risk assessment, compensating controls and approval from the designated authority.
- This Policy shall be reviewed annually or whenever significant changes occur in business operations, applicable regulations, technology, or information security risks to ensure its continued suitability, adequacy and effectiveness.