SPORTS AUTHORITY OF INDIA
IT DIVISION

RISK MANAGEMENT POLICY

Document No.: 01-01023(23)/1/2026-IT(HO)
Version: 1.0
Document Type: Internal Policy
Effective Date: 28.10.2026
Document Owner: IT Division, **Sports Authority of India**
Review Frequency: Annual

---

1. PURPOSE

The purpose of this Risk Management Policy is to establish a structured and consistent approach for identifying, assessing, evaluating, treating, monitoring, and reviewing risks that may impact the confidentiality, integrity, availability, regulatory compliance, operational continuity, reputation, and business objectives of **SAI**.

This Policy aims to ensure that risks are identified and managed proactively to support informed decision-making, strengthen organizational resilience, and maintain compliance with applicable legal, regulatory, and information security requirements.

---

2. SCOPE

This Policy applies to:

- All employees, contractual personnel, consultants, interns, and third-party service providers.
- All business processes, projects, systems, applications, facilities, information assets, and operational activities.
- Information security, cyber security, operational, legal, regulatory, privacy, third-party, and technology-related risks.
- All departments and units within **SAI**.

---

3. OBJECTIVES

The objectives of this Policy are to:

- Identify and manage risks systematically.
- Protect organizational information assets and critical operations.
- Reduce the likelihood and impact of adverse events.
- Support business continuity and resilience.
- Ensure compliance with applicable laws and regulations.

- Facilitate risk-based decision making.
- Promote a culture of proactive risk management.

4. REFERENCE DOCUMENTS AND APPLICABLE REQUIREMENTS

This Policy shall be read in conjunction with:

- Information Technology Act, 2000.
- Digital Personal Data Protection Act, 2023.
- CERT-In Directions dated 28 April 2022.
- CERT-In Guidelines on Information Security Practices for Government Entities (CISG-2023-01).
- MeitY Guidelines on Information Security Practices for Government Entities.
- ISO/IEC 27001:2022.
- ISO/IEC 27005:2022 – Information Security Risk Management.
- ISO 31000:2018 – Risk Management Guidelines.
- NIST Cybersecurity Framework (CSF 2.0).

5. DEFINITIONS AND ABBREVIATIONS

Term	Definition
Risk	The effect of uncertainty on objectives
Threat	Potential cause of an unwanted incident
Vulnerability	Weakness that can be exploited by a threat
Risk Assessment	Process of identifying and evaluating risks
Risk Treatment	Process of modifying risk through controls
Residual Risk	Risk remaining after implementation of controls
Risk Owner	Individual accountable for management of a risk
Risk Register	Central repository of identified risks

6. ROLES AND RESPONSIBILITIES

6.1 Management

Management shall:

- Approve the Risk Management Framework.
- Provide resources necessary for risk management.

- Review significant risks periodically.
- Support implementation of risk treatment plans.

6.2 Risk Management Committee

The Risk Management Committee shall:

- Oversee risk management activities.
- Review organizational risk posture.
- Escalate significant risks to management.
- Ensure effective implementation of risk treatment plans.

6.3 IT Division

The IT Division shall:

- Conduct risk assessments for information systems.
- Monitor cyber security risks.
- Maintain risk assessment records.
- Recommend risk treatment measures.
- Review effectiveness of implemented controls.

6.4 Risk Owners

Risk Owners shall:

- Identify and assess risks.
- Implement risk treatment measures.
- Monitor assigned risks.
- Report risk status periodically.

6.5 Employees and Users

All personnel shall:

- Report identified risks and security concerns.
- Follow approved risk management procedures.
- Cooperate during risk assessments.

---

7. RISK MANAGEMENT PRINCIPLES

SAI shall ensure that:

- Risk management is integrated into organizational processes.
- Risk decisions are based on documented assessments.
- Risk treatment measures are proportional to identified risks.

- Risks are regularly monitored and reviewed.
- Continuous improvement is maintained.

---

8. RISK IDENTIFICATION

Risks shall be identified through:

- Risk assessments.
- Vulnerability assessments.
- Security audits.
- Compliance reviews.
- Incident investigations.
- Threat intelligence.
- Business continuity activities.
- Third-party assessments.
- Change management activities.

Risk identification shall consider internal and external factors that may affect organizational objectives.

---

9. RISK CATEGORIES

The organization shall assess risks including but not limited to:

9.1 Information Security Risks

- Unauthorized access
- Data breaches
- Malware attacks
- Ransomware incidents

9.2 Operational Risks

- Process failures
- Human errors
- Resource constraints

9.3 Technology Risks

- Infrastructure failures
- Software vulnerabilities
- System outages

9.4 Third-Party Risks

- Vendor failures
- Supply chain risks
- Outsourcing risks

9.5 Compliance Risks

- Regulatory violations
- Legal non-compliance
- Audit findings

9.6 Business Continuity Risks

- Natural disasters
- Facility disruptions
- Service interruptions

---

10. RISK ASSESSMENT

Risk assessments shall evaluate:

- Likelihood of occurrence.
- Potential business impact.
- Existing controls.
- Regulatory implications.
- Financial implications.
- Reputational impact.

Risk assessments shall be conducted:

- Annually.
- Before implementation of major changes.
- For new projects and systems.
- After significant incidents.

Where SAI operates or supports an Aadhaar authentication application under an applicable UIDAI arrangement, an information security risk assessment of the supporting ICT infrastructure shall be conducted at least annually, or at such frequency as may be prescribed by applicable requirements. The assessment shall include relevant third-party suppliers and service providers, identify material risks and vulnerabilities, and record risk treatment measures, responsible persons and target completion dates.

11. RISK ANALYSIS

Risks shall be analyzed using a documented methodology considering:

- Threat capability.
- Vulnerability severity.
- Asset value.
- Exposure level.
- Business dependency.

Risk ratings shall be assigned using approved risk scoring criteria.

---

12. RISK EVALUATION

Identified risks shall be categorized as:

Risk Level	Description
Critical	Immediate treatment required
High	Urgent remediation required
Medium	Planned mitigation required
Low	Acceptable with monitoring

Management shall review significant and critical risks regularly.

---

13. RISK TREATMENT

Risk treatment options may include:

Risk Mitigation

Implementation of security controls to reduce risk.

Risk Avoidance

Discontinuing activities causing unacceptable risk.

Risk Transfer

Transferring risk through insurance or contractual arrangements.

Risk Acceptance

Formally accepting risk with management approval.

All treatment decisions shall be documented.

---

14. RISK ACCEPTANCE

Residual risks exceeding defined thresholds shall:

- Be documented.
- Include business justification.
- Be approved by authorized management.
- Be periodically reviewed.

Risk acceptance shall not override legal or regulatory requirements.

---

15. RISK REGISTER MANAGEMENT

SAI shall maintain a Risk Register containing:

- Risk identifier.
- Risk description.
- Risk owner.
- Impact rating.
- Likelihood rating.
- Risk score.
- Treatment plan.
- Residual risk.
- Review status.

The Risk Register shall be updated periodically.

---

16. THIRD-PARTY RISK MANAGEMENT

Third-party risks shall be assessed considering:

- Information access.
- Data processing activities.
- Cyber security maturity.
- Regulatory obligations.
- Business dependency.

Critical vendors shall be reviewed periodically.

---

17. INFORMATION SECURITY RISK MANAGEMENT

Information security risks shall be managed through:

- Access controls.
- Network security measures.

- Encryption controls.
- Vulnerability management.
- Patch management.
- Incident management.
- Security monitoring.

---

18. BUSINESS CONTINUITY RISK MANAGEMENT

Critical business processes shall undergo risk assessments to:

- Identify disruption scenarios.
- Determine recovery requirements.
- Support continuity planning.
- Strengthen resilience capabilities.

---

19. RISK MONITORING AND REVIEW

Risks shall be monitored through:

- Risk reviews.
- Internal audits.
- Security assessments.
- Compliance reviews.
- Incident trend analysis.
- Management reviews.

Risk status shall be reported periodically.

---

20. TRAINING AND AWARENESS

SAI shall conduct awareness programs covering:

- Risk identification.
- Security risks.
- Compliance obligations.
- Reporting responsibilities.
- Risk treatment processes.

Training records shall be maintained.

---

21. COMPLIANCE AND MONITORING

Compliance with this Policy shall be monitored through:

- Internal audits.
- External audits.
- Risk assessment reviews.
- Compliance assessments.
- Management reporting.

Non-compliance may result in corrective actions and disciplinary measures.

---

22. EXCEPTION MANAGEMENT

Any exception to this Policy shall:

- Be documented.
- Be risk assessed.
- Include compensating controls where applicable.
- Be approved by competent authority.
- Be periodically reviewed.

---

23. POLICY REVIEW

This Policy shall be reviewed:

- At least annually.
- Following significant security incidents.
- Following major organizational changes.
- Following regulatory updates.
- Following audit observations.

---

24. EFFECTIVE DATE

This Policy becomes effective on 27.10.2026 by the approval by the Competent Authority and shall remain in force until amended, replaced, or withdrawn.

---

25. APPROVAL

This Risk Management Policy is approved by the Competent Authority of **SAI** and shall be implemented across the organization.

---

26. REFERENCES

The following documents, standards, guidelines, and regulatory requirements were referred to while preparing this Policy:

1. **Information Technology Act, 2000**
   Link: https://www.meity.gov.in
2. **Digital Personal Data Protection Act, 2023**
   Link: https://www.meity.gov.in
3. **CERT-In Directions under Section 70B dated 28 April 2022**
   Link: https://www.cert-in.org.in/Directions70B.jsp
4. **CERT-In Guidelines on Information Security Practices for Government Entities (CISG-2023-01)**
   Link: https://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=CISG-2023-01
5. **MeitY Guidelines on Information Security Practices for Government Entities**
   Link: https://www.meity.gov.in
6. **ISO/IEC 27001:2022 Information Security Management Systems**
   Link: https://www.iso.org/isoiec-27001-information-security.html
7. **ISO/IEC 27005:2022 Information Security Risk Management**
   Link: https://www.iso.org/standard/80585.html
8. **ISO 31000:2018 Risk Management Guidelines**
   Link: https://www.iso.org/iso-31000-risk-management.html
9. **NIST Cybersecurity Framework (CSF 2.0)**
   Link: NIST CSF

Chattopadhyay

***