Approved By	Controlled By
HOD(C&IT)	CISO

Document Name	Risk Assessment and Treatment Methodology
Document Version	1.0
Document ID	ISMS/DOC/Procedures/18
Security Classification	Public
Review Frequency	Annually
Date	19.05.2025

Document Change Record

Version History:

Sl. NO.	Version	Issue Date	Prepared By	Reviewed By	Approved By	Change Description
1.	1.0	19.05.2025	Shweta Roy Sr. Mgr (C&IT) 19.05.2025	A K Choudhry CISO, GM(C&IT) 19.05.2025	Rajan Kumar CGM (C&IT) 19.05.2025	Initial Release

Distribution List:

- C&IT Department
- ISMS Security Forum

Notes:

- This is a controlled document under ISO 27001 ISMS. Unauthorized changes are prohibited.
- Ensure the most recent version is used at all times.
- All changes must be recorded in the Document Change Record section.

Purpose

This document defines the methodology for conducting information security risk assessments and implementing risk treatment for Bokaro Steel Plant's Information Security Management System (ISMS) in accordance with ISO 27001:2022 requirements.

Scope

This methodology applies to all information assets, IT infrastructure, systems, and operations within the Computer & Information Technology Department as defined in the ISMS scope. Specifically, this includes:

- Information assets (data, databases, documentation)
- IT infrastructure (servers, network devices, endpoints)
- Applications and systems
- Supporting facilities and services
- Personnel and processes

❖ Risk Assessment Process Overview

❖ The risk assessment process follows these key steps:
❖ Context establishment
❖ Risk identification
❖ Risk analysis
❖ Risk evaluation
❖ Risk treatment
❖ Risk acceptance
❖ Risk communication
❖ Risk monitoring and review

❖ Context Establishment

➢ External Context Considerations

- Regulatory environment and legal requirements
- Competitive landscape and industry standards
- Technological trends and evolving threats
- Third-party relationships and dependencies

➢ Internal Context Considerations

- Strategic objectives and business priorities
- Organizational structure and responsibilities
- Available resources and capabilities
- Existing policies, procedures, and controls
- Information security culture and awareness

➢ Risk Assessment Parameters

- Risk assessment scope and boundaries

- Risk criteria and evaluation metrics
- Roles and responsibilities
- Information sources and documentation requirements
- Assessment timeframe and frequency

❖ Risk Identification

➢ Asset Identification

- Identify and document information assets within scope
- Classify assets according to the Information Classification Policy
- Determine asset ownership and value
- Document dependencies between assets
- Assets to be identified include:
  - Primary assets:
    - ♦ Business processes and activities
    - ♦ Information and data
  - Supporting assets:
    - ♦ Hardware
    - ♦ Software
    - ♦ Network infrastructure
    - ♦ Personnel
    - ♦ Physical sites
    - ♦ Organizational structure

➢ Threat Identification

- Identify potential threats that could affect the confidentiality, integrity, or availability of assets. Threats are categorized as:
  - **Natural threats**:
    - ♦ Floods, fires, earthquakes
    - ♦ Extreme weather events
    - ♦ Pandemics or health emergencies
  - **Human threats - Unintentional**:
    - ♦ User errors and mistakes
    - ♦ Configuration errors
    - ♦ Negligence and oversight
    - ♦ Improper handling of data
  - **Human threats - Intentional**:
    - ♦ Unauthorized access
    - ♦ Malware and ransomware attacks
    - ♦ Social engineering
    - ♦ Insider threats
    - ♦ Data theft
    - ♦ Sabotage
    - ♦ Denial of service attacks

- **Technical threats**:
  - ♦ System failures
  - ♦ Hardware malfunctions
  - ♦ Software defects
  - ♦ Network outages
  - ♦ Power failures
  - ♦ Capacity issues
- **Operational threats**:
  - ♦ Process failures
  - ♦ Inadequate documentation
  - ♦ Poor change management
  - ♦ Insufficient monitoring
  - ♦ Supply chain issues

➢ Vulnerability Identification

- Identify weaknesses that could be exploited by threats, through:
- Vulnerability scanning and penetration testing
- Security assessments and audits
- Review of previous incidents
- Vendor advisories and threat intelligence
- Control effectiveness evaluations
- Compliance gap analysis
- Common vulnerabilities to consider:
- Missing security patches
- Weak authentication mechanisms
- Insecure default configurations
- Inadequate access controls
- Insufficient encryption
- Lack of security awareness
- Inadequate physical security
- Insufficient business continuity measures
- Poor coding practices

➢ Existing Controls Identification

- Document existing security controls according to ISO 27001 Annex A categories:
  - A.5: Organizational controls
  - A.6: People controls
  - A.7: Physical controls
  - A.8: Technological controls
- For each control, document:
  - Control description
  - Implementation status
  - Control owner
  - Evidence of operation

- Known weaknesses or deficiencies

❖ Risk Analysis

➢ Risk Analysis Approach

- Bokaro Steel Plant employs a semi-quantitative risk analysis approach, combining qualitative assessment with numerical values to enable prioritization.

➢ Asset Value Assessment

Assets are valued based on:

Value	Description	Criteria
5 (Very High)	Critical to operations	Complete failure would cause extreme damage to the organization
4 (High)	Vital to operations	Significant impact on core business functions
3 (Medium)	Important to operations	Moderate impact on business functions
2 (Low)	Minor importance	Limited impact on business functions
1 (Very Low)	Minimal importance	Negligible impact on business functions

➢ Threat Likelihood Assessment

Threats are assessed for likelihood of occurrence:

Value	Likelihood	Criteria
5 (Almost Certain)	Expected to occur	Multiple times per year
4 (Likely)	Will probably occur	Once per year
3 (Possible)	Might occur	Once every 1-2 years
2 (Unlikely)	Not expected to occur	Once every 2-5 years
1 (Rare)	Exceptional circumstances only	Once every 5+ years

➢ Vulnerability Assessment

Vulnerabilities are assessed for their ease of exploitation:

Value	Vulnerability Level	Criteria
5 (Very High)	Easily exploitable	No specialized skills required, public tools available
4 (High)	Moderately exploitable	Minimal specialized skills required
3 (Medium)	Somewhat exploitable	Some specialized skills required
2 (Low)	Difficult to exploit	Significant specialized skills required
1 (Very Low)	Very difficult to exploit	Highly specialized skills and resources required

➢ Impact Assessment

Impact is assessed across multiple dimensions:

Dimension	Description
Confidentiality	Unauthorized disclosure of information
Integrity	Unauthorized modification of information
Availability	Disruption of access to information or systems
Regulatory	Compliance violations and legal consequences
Reputational	Damage to organization's reputation
Financial	Direct and indirect financial losses
Operational	Disruption to business operations

Impact values:

Value	Impact Level	Description
5 (Catastrophic)	Critical impact	Severe, possibly irreversible damage; may threaten survival
4 (Major)	Significant impact	Major damage requiring substantial resources to recover
3 (Moderate)	Measurable impact	Notable damage requiring significant effort to recover
2 (Minor)	Limited impact	Minor damage with minimal recovery effort
1 (Insignificant)	Negligible impact	Minimal or no damage, routine response

➢ Risk Calculation

- Risk Level = Threat Likelihood × Vulnerability Level × Impact
- This produces a risk score ranging from 1 to 125.

➢ Inherent vs. Residual Risk

- **Inherent Risk**: The risk level without considering existing controls
- **Residual Risk**: The risk level after applying existing controls
- Control effectiveness is assessed to determine residual risk:

Value	Control Effectiveness	Description
0.9	Minimal	Controls have minimal effect on risk
0.7	Partial	Controls partially mitigate risk
0.5	Significant	Controls significantly reduce risk
0.3	Substantial	Controls substantially reduce risk
0.1	Optimal	Controls almost eliminate risk

- Residual Risk = Inherent Risk × Control Effectiveness

❖ Risk Evaluation

➢ Risk Prioritization

Risks are prioritized based on their calculated risk levels:

Risk Level	Range	Response
Critical	75-125	Immediate attention and remediation required
High	50-74	Prompt attention and timely remediation required
Medium	25-49	Planned attention and scheduled remediation
Low	10-24	Routine management and monitoring
Very Low	1-9	Acceptance with minimal monitoring

➢ Risk Register

- All identified risks shall be documented in the Risk Register, which includes:
  - Risk ID and description
  - Affected assets
  - Threat and vulnerability details
  - Inherent risk score
  - Existing controls
  - Residual risk score
  - Risk owner
  - Treatment plan
  - Status and review dates

❖ Risk Treatment

➢ Risk Treatment Options

- Four options for risk treatment:
  - **Risk Modification (Mitigation)**: Implement controls to reduce risk to an acceptable level
    - ♦ Technical controls
    - ♦ Administrative controls
    - ♦ Physical controls
    - ♦ Combination of control types
  - **Risk Retention (Acceptance)**: Accept the risk without further action
    - ♦ Documented formal acceptance
    - ♦ Monitoring requirements
    - ♦ Annual review requirements
  - **Risk Avoidance**: Eliminate the risk by removing the risk source
    - ♦ Cease activity
    - ♦ Change process
    - ♦ Remove asset
  - **Risk Sharing (Transfer)**: Transfer risk to another party
    - ♦ Insurance
    - ♦ Outsourcing
    - ♦ Contractual agreements

➢ Risk Treatment Plan

- For each risk requiring treatment, develop a treatment plan that includes:
  - Selected treatment option(s)
  - Required controls or actions
  - Resources required
  - Responsibilities
  - Implementation timeline
  - Success metrics
  - Monitoring requirements

➢ Control Selection

- Controls should be selected based on:
- Effectiveness in addressing risk
- Cost-benefit analysis
- Implementation feasibility
- Operational impact
- Compliance requirements
- Integration with existing controls
- Reference ISO 27001:2022 Annex A for control selection.

➢ Statement of Applicability

- Document selected controls in the Statement of Applicability (SoA), which identifies:
- Applicable ISO 27001:2022 controls
- Implementation status
- Justification for inclusion or exclusion
- Implementation details

❖ Risk Acceptance

➢ Risk Acceptance Levels

Risk acceptance authority based on risk level:

Risk Level	Acceptance Authority
Critical	Executive Management / Board
High	Department Director / CISO
Medium	Information Security Manager
Low	System Owner / Process Owner
Very Low	System Owner / Process Owner

➢ Risk Acceptance Process

- Document risks for acceptance in the Risk Acceptance Form
- Provide justification for acceptance
- Submit for approval to appropriate authority
- Document acceptance decision in Risk Register
- Implement monitoring requirements

- Schedule periodic review

❖ Risk Communication and Consultation

➢ Internal Communication

- Regular risk reports to management
- Risk awareness training for staff
- Inclusion of risk topics in security briefings
- Consultation with stakeholders during risk assessment

➢ External Communication

- Notification to relevant external parties when required
- Regulatory reporting as required
- Communication with third parties regarding shared risks

➢ Risk Reporting

- Risk reports shall include:
- Summary of risk profile
- Significant changes to risk landscape
- Status of risk treatment plans
- Risk acceptance decisions
- Emerging risks

❖ Risk Monitoring and Review

➢ Monitoring Activities

- Continuous monitoring of high-risk areas
- Regular review of risk indicators
- Effectiveness assessment of controls
- Compliance monitoring
- Incident analysis

➢ Review Frequency

Risk reviews shall be conducted:

Risk Level	Review Frequency
Critical	Monthly
High	Quarterly
Medium	Semi-annually
Low	Annually
Very Low	Annually

➢ Triggers for Reassessment

- Significant organizational changes
- Major system changes
- New or modified business processes
- Security incidents
- Changes in threat landscape
- New vulnerabilities

- Regulatory changes
- Third-party changes

❖ Risk Assessment Documentation

➢ Required Documentation

- Risk Assessment Plan
- Risk Register
- Risk Treatment Plan
- Risk Acceptance Records
- Statement of Applicability
- Risk Monitoring Reports

➢ Documentation Retention

- Risk assessment documentation shall be retained for at least three years or as required by applicable regulations.

❖ Roles and Responsibilities

➢ Executive Management

- Approve risk methodology
- Provide resources for risk management
- Accept high-level risks
- Review and approve risk reports

➢ Risk Manager

- Develop and maintain risk methodology
- Coordinate risk assessments
- Facilitate risk treatment decisions
- Report on risk management activities

➢ Information Security Manager

- Provide security expertise
- Support risk assessment activities
- Recommend security controls
- Monitor control effectiveness

➢ System/Asset Owners

- Identify assets
- Participate in risk assessments
- Implement risk treatments
- Accept lower-level risks

➢ Process Owners

- Identify process risks
- Implement process controls
- Monitor process-related risks

➢ IT Personnel

- Provide technical expertise
- Implement technical controls

- Monitor technical risks

❖ Methodology Review

- This methodology shall be reviewed:
  - Annually
  - After significant organizational changes
  - After major security incidents
  - When new threats or vulnerabilities emerge
  - When risk assessment results indicate ineffective methodology

END OF DOCUMENT