

Risk Assessment Policy

(Classification and Handling -Safeguarding Sensitive and Confidential Information)

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party.

Version:1

DOCUMENT HISTORY

VERSION NO.	REVISION DATE	AUTHOR	REVIEWED BY	APPROVED BY	DESCRIPTION
1	01/01/2025	Gyan Singh	Mr.P.Sahoo	Mr.Amit Sobti	Approved

A **Risk Assessment Policy** sets the foundation for the organization's approach to risk management and is designed to ensure that risks are identified, assessed, managed, and monitored in a structured and consistent manner.

Key Elements of the Risk Assessment Policy:

1. Purpose and Scope

- The purpose of the policy is to define the risk management approach and to ensure the identification, evaluation, and treatment of cybersecurity risks across the organization.
- The policy applies to all information systems, assets, and processes that could impact the organization's security posture.

2. Risk Management Principles

- Risk assessments should be conducted based on the following principles:
 - **Proportionality:** Risk treatment should be proportional to the risk's potential impact.
 - **Transparency:** Risk assessment results should be clear and understandable to stakeholders.
 - **Ongoing Process:** Risk assessments are not one-time events but an ongoing part of the organization's operations.

3. Risk Assessment Methodology

- The organization follows the ISO/IEC 27001 standard for risk assessment methodology, which typically includes identifying risks, evaluating their potential impact, assessing the likelihood, and determining how to treat the risks.
- A common risk assessment methodology may involve qualitative and quantitative approaches, risk matrices, and predefined criteria for likelihood and impact.

4. Roles and Responsibilities

- **Risk Management Team:** A cross-functional team responsible for performing risk assessments and recommending risk treatments.
- **Business Units:** Responsible for providing input on business-specific risks and supporting the risk treatment process.

5. Risk Assessment Frequency

- Risk assessments will be conducted annually and whenever significant changes to systems, processes, or technologies occur. Emergency or ad-hoc assessments may also be performed if significant risks or vulnerabilities are identified (e.g., after a cyber attack or a major system failure).

6. Risk Acceptance and Treatment

- Risks identified will be classified into categories: **acceptable**, **tolerable**, or **unacceptable**. For acceptable risks, no immediate action may be required. Unacceptable risks will be mitigated through appropriate controls. Tolerable risks will be monitored over time.

Risk Assessment Procedures

The **Risk Assessment Procedure** outlines the step-by-step process for performing risk assessments and managing the identified risks.

Key Steps in the Risk Assessment Procedure:

1. Preparation for Risk Assessment

- **Define Scope:** Identify the systems, assets, and processes to be assessed.
- **Gather Information:** Collect information about assets, threats, vulnerabilities, and existing security controls.
- **Identify Stakeholders:** Identify the key stakeholders involved in the risk assessment, including business units, IT, and compliance teams.

2. Risk Identification

- **Asset Identification:** Identify the critical assets (e.g., hardware, software, data) and their value to the organization.
- **Threat Identification:** Identify potential threats (e.g., cyber-attacks, natural disasters, insider threats) that could impact the organization.
- **Vulnerability Identification:** Identify weaknesses in systems or processes that could be exploited by threats.
- **Impact Analysis:** Analyze the potential impact of a threat exploiting a vulnerability (e.g., financial loss, reputational damage).

3. Risk Evaluation

- **Likelihood and Impact Assessment:** Evaluate the likelihood of each identified risk and the potential impact it would have on the organization. This is typically done using risk matrices (e.g., low, medium, high) to prioritize risks.
- **Risk Rating:** Each risk is rated based on likelihood and impact, resulting in a risk score or classification (e.g., low, medium, high).
- **Risk Appetite:** Compare the evaluated risks with the organization's risk appetite (the level of risk the organization is willing to accept).

4. Risk Treatment

- **Mitigation Controls:** Identify appropriate controls or countermeasures to reduce the risk (e.g., technical controls like firewalls, administrative controls like employee training, physical controls like secure access).
- **Risk Transfer:** Determine if any risks can be transferred (e.g., through insurance or outsourcing).
- **Risk Acceptance:** For low-priority risks, determine if the organization will accept the risk without additional controls.

5. Implementation of Controls

- Implement the selected risk treatment controls and ensure they are effective.
- Ensure all control measures are documented and aligned with the risk treatment plan.

6. Monitor and Review

- **Continuous Monitoring:** Continuously monitor the effectiveness of implemented controls.
- **Periodic Reviews:** Review the risk treatment plan at regular intervals (e.g., annually) or after major changes to assess whether risks have changed and if additional actions are needed.

7. Communication and Reporting

- **Documentation:** Document the entire risk assessment process, findings, and decisions.
- **Reporting:** Communicate the risk assessment results to senior management and relevant stakeholders. This helps ensure that risks are managed at the appropriate levels and that the risk treatment plans are followed.