Risk Assessment Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Risk assessments help identify business processes that are of high priority and importance to the organization so the proper controls can be implemented to reduce risks to acceptable levels.

# II. Purpose

Information Resources are critical to maintaining ABC Company’s business operations. This policy ensures sufficient controls and resources are allocated to supporting and managing IT and its use within ABC Company.

# III. Scope

This policy applies to all ABC Company Staff that have access to ABC Company’s Information Resources.

# IV. Policy

A. Risk Assessments

Risk assessments identify ABC Company Information Resources and related threats and vulnerabilities. The accompanying risk analysis identifies the impact on our organization and provides recommendations for treating risks.

To properly secure and protect ABC Company’s Information Resources, a significant amount of design, planning, and implementation expertise is required to ensure that the proper level of controls are designed and implemented. While preparing and conducting a risk assessment, the following best practices or approaches should be considered.

ABC Company’s Risk Management Officer (RMO) shall first define the risk assessment’s goals and objectives. Aligning these goals and objectives with the organization’s business drivers allows the organization to prioritize and focus on critical systems and assets.

ABC Company staff shall identify and inventory important Information Resource assets and related components. Without an accurate inventory of infrastructure components and IT assets, an asset valuation, criticality, or importance evaluation cannot be performed.

Depending on the accuracy and availability of inventory documentation and asset valuation data (for example, capital dollars spent on hardware, software, integration, maintenance, staff salaries, G&A overhead), ABC Company Staff should conduct an asset valuation or asset criticality (importance) assessment to prioritize and determine which IT infrastructure components and assets are most important to the organization (either in monetary value or importance value).

Depending upon the scope of the risk assessment, ABC Company management may or may not be faced with a limited budget to conduct a thorough risk and vulnerability assessment. In some cases, the organization may limit the scope to mission-critical IT infrastructure components and assets only.

The risk assessment shall identify assets, threats to the assets, vulnerabilities that exist as a result of the threats, and likelihood of the event. Charts or other documents shall describe how sensitive information is created, received, maintained, transmitted, and flows through the organization. Such documentation shall consider and identify:

* Less obvious sources of sensitive information including mobile devices.
* External sources including vendors, consultants, and other third party service providers that create, receive, maintain, or transmit sensitive information.

For third party service providers, at a minimum, the risk assessment shall:

* Be performed on an annual basis or more frequently if major changes occur to the environment or services performed.
* Identify compliance objectives and control requirements.
* Identify risks related to business continuity, capacities, and dependent services.

B. Risk Analysis

After the assets, threats, and vulnerabilities have been identified, the RMO shall ensure a risk analysis identifies the impact on ABC Company’s Information Resources. By aligning the potential risks, threats, and vulnerabilities to the prioritized assets, management can make sound business decisions based on the value or criticality of that IT asset and the potential risk, threats, and vulnerabilities that are known.

The risk analysis shall include a Risk Treatment Plan that identifies how each of ABC Company’s risks can be managed:

* Mitigate – implement controls to reduce risks to an acceptable level.
* Transfer – transfer risks to another entity (usually through insurance).
* Avoid – change the business model to avoid or eliminate the risk if the risk cannot be reduced to an acceptable level or transferred to another entity.
* Monitor – acknowledge the risk and monitor to ensure the risk remains within acceptable limits.

C. Risk Treatment Plan

The Risk Treatment Plan shall include a prioritized list of assets, related vulnerabilities, and preventive, detective, and corrective controls that manage risks. The prioritized list helps align allocation of funds based upon criticality of the asset and related risks.

To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be located away from locations subject to high probability environmental risks.

Redundant equipment shall be located a reasonable distance away from primary systems.

For third party service providers, the risk analysis and risk treatment plan shall:

* Identify measures in place to protect Sensitive Information and provide services as outlined in the agreement with the service provider.
* Evaluate risks and ensure controls are in place to treat risks.
* Identify gaps from compliance objectives and control requirements. Make service provider aware of such gaps and take appropriate actions necessary.

Executive management shall be involved in risk management and mitigation decisions including how security processes are communicated throughout the organization. The risk assessment, risk analysis, and risk treatment plan shall be reviewed on an annual basis to ensure that controls are sufficient and effective at treating risks.

The Chief Security Officer (CSO) shall ensure:

* Security measures protect electronically transmitted sensitive information is not improperly modified without detection.
* The risk assessment identifies scenarios that may result in modification to sensitive information by unauthorized sources during transmission.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all Staff members with access to ABC Company’s Information Resources.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM03.02, APO01.03, APO03.06, APO12.02, APO12.07, APO13.07, DSS05.02

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B)

ISO 27001:2013 6.1.2, 6.1.3, 8.2, 8.3, 9.3

NIST SP 800-37 3.2, 3.5, 3.7

NIST SP 800-53 3.17 (RA-1-9), SI-2, SI-4

NIST Cybersecurity Framework ID.RA-1-6, ID.RM-1, ID.SC-4, DE.CM-1-6, RS.RP-1, RS.MI-2

PCI 6.1, 10.6.2, 10.8.1, 12.2