Risk Management 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 management is an on-going process by which ABC Company Staff manage risks through a three-step process:

* Risk Assessment – Identify assets, threats to the assets, and vulnerabilities that exist as a result of the threats.
* Risk Analysis – For each risk, identify the likelihood and impact on our organization.
* Risk Treatment Plan – Develop controls and other safeguards designed to mitigate, eliminate, or transfer risks. It is important to treat risks in a cost effective and efficient manner.

# II. Purpose

This policy establishes the framework for a formal risk management program by establishing responsibility for risk identification, analysis, and risk treatment. Risk management is an enterprise-wide activity that applies to all ABC Company departments.

# III. Scope

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

# IV. Policy

Risk is the potential that a threat will exploit one or more asset vulnerabilities and result in a loss or failure to achieve an objective. At ABC Company, risk management is the process of identifying, analyzing, and the use of safeguards and controls to treat risks.

Where possible, ABC Company shall modify or eliminate conditions and practices which may cause loss. Where risk cannot be eliminated or reduced, it shall be monitored to ensure it remains within acceptable levels.

Risk management is an important component of ABC Company’s Resilient Policy.

A. Executive Management Responsibilities

Executive management shall be involved in risk management and mitigation decisions including how security processes are communicated throughout the organization. A summary of the departmental Risk Assessment, Risk Analysis, and Risk Treatment Plans shall be reviewed by Executive Management on an annual basis to ensure that controls are sufficient and effective at treating risks. Executive Management may determine that the risks are acceptable given the kind and severity of known risks and unknown risks from the Chief Security Officer’s uncertainty analysis.

B. Risk Management Officer Responsibilities

*Risk Management Framework*

ABC Company’s Risk Management Officer (RMO) shall ensure a formal and document Risk Management Framework has been established to manage risks related to Information Systems. The Risk Management Framework shall include:

* Categorizing Information Systems
* Selecting security controls
* Implementing security controls
* Assessing security controls
* Authorizing security controls
* Monitoring security controls

Categorize. Information Systems shall be categorized based upon the potential impact to the organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories shall be used in conjunction with vulnerability and threat information in assessing the risk to an organization. The security category of an Information System shall consider the confidentiality impact, integrity impact, and availability impact where the impact is classified as Low, Medium (Moderate), High, or Not Applicable. When determining the impact level of an information system the RMO shall consider the different types of information that are processed, stored, or transmitted by the information system, the impact values (Low, Medium, High, Not Applicable), the information system security categorization, that is, the highest impact value for each security objective (confidentiality, integrity, availability) from among the categorizations for the information types associated with the information system, Determine the overall impact level of the information system from the highest impact value among the three security objectives in the system security categorization.

Select. An applicable security control baseline shall be selected based on the results of the security categorization. To adequately mitigate risk is an important task that requires a fundamental understanding of ABC Company's mission/business priorities, the mission and business functions the Information Systems support, and the environments of operation where the systems reside. In preparation for selecting and specifying the appropriate security controls for organizational Information Systems and their respective environments of operation, the RMO shall first determine the criticality and sensitivity of the information to be processed, stored, or transmitted by those systems. The RMO can employ a requirements definition approach or a gap analysis approach in selecting security controls and control enhancements to supplement initial baselines. The RMO shall document significant risk management decisions in the security control selection process so that Executive Management can have access to the necessary information to make informed authorization decisions for organizational information systems. Maintaining a record of security control selection and control status can be addressed in one or multiple documents or plans. There may be situations in which organizations cannot apply sufficient security controls within their information systems to adequately reduce or mitigate risk (e.g., when using certain types of information technologies or employing certain computing paradigms). Therefore, the RMO shall document alternative strategies to prevent organizational missions/business functions from being adversely affected. Once the impact level of the information system is determined, organizations begin the security control selection process. After selecting the applicable security controls, organizations initiate the tailoring process to modify appropriately and align the controls more closely with the specific conditions within the organization (i.e., conditions related to organizational missions/business functions, information systems, or environments of operation). The tailoring process includes:

* Identifying and designating common controls in initial security control baselines.
* Applying scoping considerations to the remaining baseline security controls.
* Selecting compensating security controls as needed.
* Assigning specific values to organization-defined security control parameters via explicit assignment and selection statements.
* Supplementing baselines with additional security controls and control enhancements, if needed.
* Providing additional specification information for control implementation, if needed.

Implement. The protection of information being processed, stored, or transmitted by information systems, seldom derives from a single safeguard or countermeasure (i.e., security control). In most cases, such protection results from the selection and implementation of a set of mutually reinforcing security controls. When considering security controls, the RMO shall consider that ABC Company is responsible and accountable for the information security risk incurred by the use of services provided by external third party service providers. Such risk shall be addressed by incorporating terms and conditions in the agreements with the external service providers. RMO baseline security control tailoring actions can include: identifying and designating common controls, applying scoping considerations, selecting compensating controls, assigning specific values to security control parameters, supplementing initial baselines with additional security controls or control enhancements, and providing additional information for control implementation. The set of security controls must be sufficient to adequately mitigate risks to organizational operations and assets, individuals, and other organizations based on the organizational risk tolerance. The RMO may find it necessary to employ compensating security controls. Compensating controls may be employed when management assesses and accepts the risk associated with implementing compensating controls in organizational information systems.

Assess. The RMO shall ensure security controls are assessed to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Two fundamental components affecting the trustworthiness of information systems are security functionality and security assurance. Security functionality is typically defined in terms of the security features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate. Security assurance is the measure of confidence that the security functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. For more information on assessing security controls please see the Audit Policy, Audit Trails Policy, Change Management Policy, and Logging Policy.

Authorize. Executive Management shall authorize Information System operation based on a determination of risk to organizational operations and assets, individuals, and other organizations resulting from the operation and use of the Information System and the decision that this risk is acceptable.

Monitor. The RMO shall ensure monitoring of the security controls in the Information System and environment of operation on an on-going basis to determine control effectiveness, changes to the system/environment, and compliance to policies, legislation, and standards. For more information on security controls see Security Controls Review Policy. Security controls shall be carefully reviewed and revised periodically to reflect:

* Experience gained from using the controls.
* Control effectiveness.
* Changes to the system/environment.
* Compliance to policies, legislation, and standards.
* Changing security requirements.
* Emerging threats, vulnerabilities, and attack methods.
* Availability of new technologies.

*Risk Management Processes*

An effective risk management process identifies, mitigates as deemed necessary, and monitors on an on-going basis, risks arising from its information and Information Systems. Risk management processes shall be integrated throughout the organization to effectively address mission/business concerns. A three-tiered approach shall be employed that addresses risk at the organization level, mission/business process level, and the information system level.

The RMO’s responsibilities include:

* Policies – Developing, implementing, and maintaining risk management policies, procedures, and guidelines.
* Management – Managing the risk management program that includes Risk Assessments, Risk Analysis, and Risk Treatment Plans.
* Approval – Approving departmental Risk Assessment, Risk Analysis, and Risk Treatment Plans.
* Security – Forwarding departmental Risk Assessment, Risk Analysis, and Risk Treatment Plans to the Chief Security Officer for review and approval.
* Reporting – Provide necessary reporting to ABC Company’s Executive Management.

The Risk Management Officer shall review department head Risk Assessments, Risk Analysis, and Risk Treatment Plans to ensure:

* The Risk Assessment produces meaningful output that reflects what is truly important to the Company.
* Asset valuation appears to be appropriate and includes the value of information, software, personnel, hardware, and physical assets (e.g. data centers). The value of an asset consists of its intrinsic value as well as the consequences of loss of asset availability, confidentiality, and integrity.
* For systems under consideration or development, risks related to existing ABC Company’s systems.
* Security controls have been identified and reduce risk to acceptable levels. Although there is flexibility in how the Risk Assessment is conducted, the process of treating risks has greater flexibility than the sequence of events conducted in a Risk Assessment.

B. Department Head Responsibilities

1. Risk Assessment

Each Department Head shall ensure that a risk assessment is performed that identifies departmental and, where appropriate, organizational assets, owners of the assets, and opportunities. The risk assessment shall identify threats to the assets and vulnerabilities that exist as a result of the threats. The Risk Assessment shall be performed on an annual basis and updated as needed. Refer to the Risk Assessment Policy for more information.

2. Risk Analysis

After the assets, threats, and vulnerabilities have been identified, Department Heads shall conduct a risk analysis that evaluates the likelihood of vulnerabilities and impact on the department and organization given the value of the specific asset and/or related resources. Department Heads shall consider the impact or lost value if the asset has been lost, disclosed, or compromised. By aligning the potential risks, threats, and vulnerabilities to the prioritized assets, Department Heads can make sound business decisions based on the value or criticality of that IT asset and the potential risk, threats, and vulnerabilities.

3. Risk Treatment Plan

Department Heads shall prepare a Risk Treatment Plan that identifies how each of the 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.

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. The Risk Treatment Plan shall identify specific tasks (Risk Task List), resources required, and estimated completion dates.

Department Heads shall consider activities and controls that help mitigate risk. Consult with appropriate security Staff (IT, CSO, physical security) to identify appropriate controls to treat risks. When selecting the appropriate controls, the following factors must be considered:

* ABC Company policies and procedures, compliance requirements, and legislation
* Technical requirements
* Safety, reliability, and quality requirements
* System performance requirements

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 cloud computing services the risk analysis and risk treatment plan shall:

* Manage risk as defined in the master agreement or industry best practices and standards.
* Identify security measures in place to protect sensitive information.

Department Heads shall:

* Monitor Risk Task List progress and update the Risk Treatment Plan as necessary.
* Submit the Risk Assessment, Risk Analysis, and Risk Treatment Plan to the Risk Management Officer for review and approval.

C. Chief Security Officer Responsibilities

The CSO shall ensure the Risk Assessment identifies scenarios that may result in modification to sensitive information by unauthorized sources during collection, storage, and transmission. Security measures shall ensure sensitive information is not improperly modified without detection.

When appropriate, the CSO shall prepare and document an uncertainty analysis for the Risk Management Officer. The uncertainly analysis shall consider a lack of sufficient information to determine the exact value of the elements of the risk model, such as threat frequency, safeguard effectiveness, or consequences.

# V. Enforcement

Any Staff 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 ABC Company Department Heads, the Risk Management Officer, and the Chief Security Officer.

**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 24

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

ISO 27001:2013 6.1.2, 8.2

NIST SP 800-37 2.2, 3.1-7

NIST SP 800-53 3.17

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, 12.2, PCI Software Security Framework