[Entity] Information Technology Standard	No:
IT Standard: **Information Security Risk Management**	Updated:
	Issued By: Owner:

1.0 Purpose and Benefits

Risk management is a critical component of any information security program. It helps ensure that any risk to confidentiality, integrity, and availability is identified, analyzed, and maintained at acceptable levels. Risk assessments allow management to prioritize and focus on areas that pose the greatest impact to critical and sensitive information assets. This provides the foundation for informed decision-making regarding information security.

Federal and State mandates require routine assessments to identify risk and ensure appropriate controls. Risk assessments allow alignment of information security with business objectives and regulatory requirements. Identifying information security risk and considering control requirements from the onset is essential, and far less costly than retrofitting or addressing the impact of a security incident.

This standard provides a risk management framework to evaluate current security posture, identify gaps, and determine appropriate actions.

2.0 Authority

[Entity Authority Needed]

3.0 Scope

[Entity Scope Needed]

4.0 Information Statement

Information security risk management takes into account vulnerabilities, threat sources, and security controls that are planned or in place. These inputs are used to determine the resulting level of risk posed to information, systems, processes, and individuals that support business functions.

While risk management and related assessment activities can take many forms (e.g., formal risk assessment, audits, security reviews, configuration analysis, vulnerability scanning and testing), all are aimed at the same goal - identifying and acting on risk to improve overall security posture.

It should be noted that an entity can never completely eliminate risk, but can take steps to manage risk.

As per the Information Security Policy, any system or process that supports business functions must be appropriately managed for risk and undergo risk assessments as part of its life cycle.

4.1 Risk Management Process

The risk management process is iterative and should be followed throughout a system's or process's life cycle.

4.1.1 Frame Risk

The first step in managing risk is to:

a. develop a strategy for conducting your risk assessment which considers assumptions, constraints, priorities, dependencies, tradeoffs and resources that will be used; and

b. determine the risk tolerance, or the level of risk that is acceptable. For information security risk decisions that may affect multiple entities, the lowest level of risk tolerance for those entities must prevail. It is important that entities recognize how fundamental this decision is to the risk management process. Risk tolerance is an executive-level decision and information technology (IT) staff should not be determining the risk tolerance for an entity.

4.1.2 Assess Risk

Assessing risk starts with identifying and classifying assets within scope. Risk is assessed by determining the threats and vulnerabilities to these assets, identifying the potential impact of each vulnerability being exploited, and determining the likelihood of occurrence. A list of potential threats and vulnerabilities needs to be developed, and may come from preexisting resources.

It is important to note that the risk assessment process is comprehensive by intention, to assure due diligence, compliance, and proper documentation of security related controls and considerations.

Designing security into systems requires an investment of time and resources. The extent of the risk assessment should be commensurate with the classification (information sensitivity and system criticality) of the system/process and the risks this system/process introduces into the overall environment.

Types of information security risk assessments include, but are not limited to:

- Enterprise Risk Assessments – Assesses risks to core agency assets, operational processes, and functions;
- Physical Infrastructure Assets and Systems Risk Assessments – Identifies and assesses vulnerabilities and risks to core physical infrastructure assets and systems;
- Project Security Risk Assessments (New Risks) – Identifies and assesses new risks to existing components introduced by new technology or service offerings; and
- Change Request Risk Assessments – Assesses risk of change to ensure security is not compromised by the proposed change.

4.1.3 Respond to Risk

Once risk has been assessed, the entity must determine and implement the appropriate course of action. Options include:

a. Risk Acceptance – This is a documented decision not to act on a given risk at a given time and place. It is not negligence or "inaction" and can be appropriate if the risk falls within the risk tolerance level. For example, entities may choose to accept the risk of an earthquake, based on a low likelihood in the Northeast of extensive damage and the high cost of controls.

b. Risk Avoidance – These are specific actions taken to eliminate the activities or technologies that are the basis for the risk. This is appropriate when the identified risk exceeds the risk tolerance, even after controls have been applied (i.e., residual risk). For example, if a connection between two networks includes unacceptable risks and the countermeasures are not practical, the entity may decide not to make the connection.

c. Risk Mitigation/Reduction – These are specific actions taken to eliminate or reduce risk to an acceptable level. This is the most common approach and is appropriate where controls can reduce the identified risk. For example, to reduce the risk of network intrusion, an entity may choose to deploy a firewall.

d. Risk Transfer/Sharing – These are specific actions taken to shift responsibility for the risk, in whole or in part, to a third party. This may be appropriate when it is more cost effective to transfer the risk, or when a third party is better suited to manage the risk. For example, an entity may transfer risk through legal disclaimers or by outsourcing to a vendor.

4.1.4 Monitor Risk

The entity must monitor the effectiveness of its risk response measures, by verifying that the controls put in place are implemented correctly and operating as intended. This must occur annually, at a minimum. In addition, the entity must have a process to alert it of significant changes in the factors it uses to assess its risk (e.g., assets, threats, controls, regulations, policies, risk tolerance). These changes may indicate a new assessment is needed.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

6.0 Definitions of Key Terms

Term	Definition

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:
[Entity Address]

8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	**Description of Change**	**Reviewer**

9.0 Related Documents

NIST SP 800-30, Guide for Conducting Risk Assessments

NIST SP 800-39, Managing Information Security Risk