	Georgia Technology Authority	
Title:	**Risk Management Framework**	
PSG Number:	**SS-08-041**	
Effective Date:	**03/31/2008**	**Review Date: 05/05/2023**
Synopsis:	Adopts the risk management framework developed by NIST for managing risk and implementing security	

PURPOSE

Risk management is an aggregation of three processes; risk assessment, risk mitigation, controls evaluation and assessment that help agencies ensure that information security management processes are integrated with agency strategic and operational planning processes. Managing risk safeguards the mission of the organization and provides an ongoing evaluation and assessment of IT-related mission risks.

This enterprise standard, consistent with the Federal Information Security Act (FISMA) of 2002, adopts the risk management framework developed by the National Institute of Standards (NIST) for assisting owners with understanding the risks associated with their decision-making processes and implementing adequate and cost-effective security.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(9) – *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(20) - *State Government, Georgia Technology, General Powers*
PM-04-001 – *Information Technology Policies, Standards and Guidelines*
PS-08-005 – *Enterprise Information Security Charter*

STANDARD

The State of Georgia shall implement a risk-based approach to information security. A successful risk management program shall have:

- Commitment from Senior management
- Full support and participation of the IT team
- A competent risk assessment team who must have the expertise to apply the risk assessment methodology to a specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization
- The awareness and cooperation of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization
- An ongoing evaluation and assessment of the IT-related mission risks

Each Agency shall use the risk management framework developed by the National Institute of Standards (NIST) for selecting and implementing security controls for its information systems as part of an organization-wide risk management program.

The framework shall be applied to both new and legacy information systems and integrated into the system development life cycle and the Enterprise Architecture.

The NIST Risk Management Framework shall include the following sequential and continuous steps (related NIST Standards and Guidelines are in parenthesis):

Step 1: Security Categorization

Categorize the information system and the information resident within that system based on the sensitivity and the impact of loss or compromise on the organization. (FIPS 199)

Step 2: Security Control Selection

Select an initial set of minimum-security controls for the information system based on the FIPS 199 security categorization and apply tailoring guidance as appropriate, to obtain a starting point for required controls. (FIPS 200 and NIST SP 800-53 Revision 1)

Step 3: Supplement Security Controls

Supplement the initial set of tailored security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances. (NIST SP 800-53)

Step 4: Document Security Controls

Document in the system security plan, the security requirements and the agreed-upon security controls planned or in place, including the organization's justification for any refinements or adjustments to the initial set of controls. (NIST SP 800-18)

Step 5: Security Controls Implementation

Implement the security controls and apply security configuration settings.

Step 6: Security Controls Assessment

Assess the effectiveness of the security controls using appropriate methods and procedures 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. (NIST SP 800-53A)

Step 7: System Authorization

Authorize information system operation based upon a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the decision that this risk is acceptable. (NIST SP 800-37)

Step 8: Controls Monitoring

Continually monitor and assess selected security controls in the information system including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis. (NIST SP 800-37 and SP 800-53A)

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Information Security – Risk Management (PS-08-031)
Information Security Infrastructure (SS-08-005)
Data Categorization – Impact Level (SS-08-014)
System Security Plans (SS-08-028)
Security Controls Review and Assessments (PS-08-029)
Independent Security Assessments (SS-08-042)

REFERENCES

NIST SP 800-12 (chapter 10) Introduction to Computer Security NIST Handbook
NIST SP 800-30 Risk Management Guide for Information Technology Systems
NIST SP 800-53/53A Security Controls and Assessing the Security Controls
NIST SP 800-18 Developing Security Plans
NIST SP 800-37 Security Certification and Accreditation
FIPS 199 Standards for Security Categorization
FIPS 200 Security Controls Standard

TERMS AND DEFINITIONS

Risk – A function of the likelihood of a given threat source exploiting a potential vulnerability, and the resulting impact of that adverse event on the organization.

Risk Management - The process of identifying, controlling and mitigating information system–related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, testing, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.

Risk Assessment - The process of identifying the risks to system security; determining the probability of occurrence, the resulting impact, and safeguards that would mitigate this impact.

Risk Mitigation – The process of prioritizing, evaluating and implementing appropriate risk-reducing controls including risk assumption, risk avoidance, risk limitation, risk planning, research and acknowledgment and risk transfer.