	Georgia Technology Authority	
Title:	**Information Security – Risk Management**	
PSG Number:	**PS-08-031**	
Effective Date:	03/20/2008	**Review Date:** 09/15/2024
Synopsis:	Requires a risk-based approach to information security management	

PURPOSE

"Risk" is the net negative impact of the exploitation of a vulnerability, considering both the probability and the impact of occurrence. "Risk management" is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. An effective risk management process is an important component of a successful IT security program and an essential management function of the organization.

The principal goal of an organization's risk management process is to protect the organization and its ability to perform its mission. It fosters informed decision-making, allowing the security management organization to balance the operation and economic costs of protective measures and achieve gains in mission capability.

This policy requires agencies to take a risk-based approach to securing their information systems.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(10) – *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(21) - *State Government, Georgia Technology, General Powers*
PM-04-001 – *Information Technology Policies, Standards and Guidelines*
PS-08-005 – *Enterprise Information Security Policy*

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, test, 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.

POLICY

Each agency shall institute an organization-wide risk management approach to information security that assesses the risks (including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction) to information and information systems that support the operations and assets of the organization.

Each agency shall develop policies, procedures and select cost-effective controls (based on the risk assessment) that reduce information security risks to an acceptable level and ensure information security is addressed throughout the lifecycle of each organization's information systems.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Information Security Infrastructure (SS-08-005)
Risk Management Framework (SS-08-041)

REFERENCES

NIST SP 800-12 AN INTRODUCTION TO INFORMATION SECURITY