

Topics:

[Risk \[2\]](#), [Disaster recovery \[3\]](#) **Risk Management Framework [1]**

SS-08-041 Risk Management Framework

Issue Date: 3/31/2008

Revision Effective Date: 3/31/2008

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 on-going 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.

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 be 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