
Topics:

[Information Security - Risk Management](#) [1]

PS-08-031 Information Security ? Risk Management

Issue Date: 3/20/2008

Revision Effective Date: 3/20/2008

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 their 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.

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, GUIDELINES

[Information Security Infrastructure \(SS-08-005\)](#) [3]

[Risk Management Framework \(SS-08-041\)](#) [4]

REFERENCES

NIST SP 800-12 (chapters 7 & 10) Introduction to Computer Security NIST Handbook

NIST SP 800-30 Risk Management Guide for Information Technology Systems

NIST SP 800-65 Integrating IT Security into the Capital Planning and Investments Controls Process

TERMS and DEFINITIONS