NIST 800 Series Information

National Institute of Standards & Technology

Overview information

The National Institute of Standards & Technology (NIST) is part of the U.S. Department of Commerce. NIST has developed dozens of standards concerning IT technology which are applicable to Federal Government institutions; many of those standards have considerable technical weight. These standards are known as the "800 series" and an index to these 800 series publications is available: **go-see-it**.

Although the intended audience for this material is IT Directors within the federal bureaucracy, we feel that some of the publications have considerable merit for companies who would like to improve their IT security profile. In that regard, the following two 800 series publications provide some risk-related definitions that are worthy of review:

800-30 **Risk Management Guide**

800-26 **Security Self-Assessment Guide for Information Technology Systems**

Interesting excerpts pertinent to IT security assurance

The following content has been extracted from the two publications listed above.

Adequate security of information and the systems that process it is a fundamental management responsibility. Agency officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

***Risk** is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.*

***Risk Management** is the ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.*

***Risk Assessment** is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system …*

*Once the risk assessment has been completed … the results should be documented in an official report or briefing. A **risk assessment report** is a management report that …. describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.*

*A **threat** is the potential for a particular threat-source to successfully exercise a particular vulnerability.*

*A **threat-source** is defined as any circumstance or event with the potential to cause harm to an IT system. A threat-source does not present a risk when there is no vulnerability that can be exercised.*

*A **vulnerability** is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.*

System and data integrity *refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality.*

System and data confidentiality *refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information …. could result in loss of public confidence, embarrassment, or legal action against the organization.*

Risk mitigation*, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.*

Audit trails *maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tolls and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.*

Agency programs must: 1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability; and 2) protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

Value [of systems and information] can be expressed in terms of the degree of sensitivity or criticality of the systems and information relative to each of the five protection categories in ….. the National Defense Authorization Act of 2000, i.e., integrity, confidentiality, availability, authenticity, and non-repudiation. [definitions follow below]

- ***Confidentiality*** - The information requires protection from unauthorized disclosure.
- ***Integrity*** - The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to:
  - ***Authenticity*** – A third party must be able to verify that the content of a message has not been changed in transit.
  - ***Non-repudiation*** – The origin or the receipt of a specific message must be verifiable by a third party.
  - ***Accountability*** - A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
- ***Availability*** - The information technology resource (system or data) must be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability also includes ensuring that resources are used only for intended purposes.

The several words in brackets "[ ]" were added by Unbeaten Path to make a quotation understandable as it stood apart from the context of the original document.

How Unbeaten Path can help (see next page)

How Unbeaten Path can help

The two products below hit the bulls-eye on the NIST recommendations quoted above.

- ☑ **Bill of Health**™ provides 50 robust assessment reports describing your iSeries security status together with a competent prescription to address each identified vulnerability. The analytical approach employed and the content of the written reports entirely fulfills NIST's "Risk Assessment" definition.
- ☑ **Stitch-in-Time**® **Data Integrity Software** quickly and decisively responds to audit challenges about the security of your data. If an unauthorized change was executed in a critical file, **Stitch-in-Time** provides comprehensive information to enable analysis of that change. The audit approach employed and the quality of the audit reports entirely fulfills NIST's "Audit Trails" definition.

Return to IT Security Assurance page