

# *NIST National Institute of Standards and Technology*

- ◆ Lets look at SP800-30 Risk Management Guide for Information Technology Systems (July 2002)
  - What follows are the NIST SP800-30 slides, which are available from the web
- ◆ Another NIST SP is the draft: Managing Risk from Information Systems: An Organizational Perspective
  - PS800-39 (April 2008)
- ◆ Source: <http://csrc.nist.gov/publications/PubsSPs.html>



## Risk Assessment Process

---

Based on recommendations of the National Institute of Standards and Technology in "Risk Management Guide for Information Technology Systems" (special publication 800-30)



## Goal of Risk Management Process

---

- Protect the organization's ability to perform its mission (not just its IT assets)
- An essential management function (not just an IT technical function)



## NIST Guide Purpose

---

- Provide a foundation for risk management program development
- Provide information on cost-effective security controls



## Guide Structure

---

- Risk Management Overview
- Risk Assessment Methodology
- Risk Mitigation Process
- Ongoing Risk Evaluation



## Risk Assessment – a definition

---

“The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.”



## Risk Assessment

---

- 1<sup>st</sup> process in risk management methodology
- Used to determine potential threats and associated risk
- Output of this process helps to identify appropriate controls to reduce or eliminate risk



## Definitions

---

- Vulnerability – weakness that can be accidentally triggered or intentionally exploited
- Threat-Source – “Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.”
- Threat – “The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.”



## Definitions

---

- Risk - "...a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization."
- Risk management – process of identifying, assessing and reducing risk



## Risk Assessment Methodology

---

- Step 1: System Characterization
  - **Input:** system-related info including
    - Hardware
    - Software
    - System interfaces
    - Data and information
    - People
    - System mission
  - **Output:**  
A good picture of system boundary, functions, criticality and sensitivity



## Risk Assessment Methodology

---

### ○ Step 2: Threat Identification

- **Input:**

- Security violation reports
- Incident reports
- Data from intelligence agencies and mass media

- **Output:**

Threat statement listing potential threat-sources (natural, human, environmental) applicable to the system being evaluated



## Risk Assessment Methodology

---

### ○ Step 3: Vulnerability Identification

- **Input:**

- System security tests (e.g. penetration tests)
- Audit results
- Vulnerability lists/advisories
- Security requirements checklist (contains basic security standards)

- **Output:**

List of system vulnerabilities (flaws or weaknesses) that could be exploited – Vulnerability/Threat pairs

## Vulnerability/Threat Pair Examples

Vulnerability	Threat-Source	Threat Action
Terminated employee ID's are not removed from the system	Terminated employees	Dialing into the company's network and accessing proprietary info
Water sprinklers used for fire suppression and no protective coverings in place	Fire; negligent persons	Water sprinklers being turned on
Vendor has identified security flaws in system and patches have not been applied	Unauthorized users (e.g. terminated employees, hackers)	Obtaining unauthorized access to sensitive files based on known vulnerabilities

## Risk Assessment Methodology

- Step 4: Control Analysis
  - **Input:** current controls, planned controls
    - Control Methods – may be technical or non-technical
    - Control Categories – preventative or detective (e.g. audit trails)
  - **Output:**
    - List of current and planned controls



## Risk Assessment Methodology

---

### ○ Step 5: Likelihood Determination

- **Input:**
  - Threat-source motivation & capability
  - Nature of the vulnerability
  - Existence & effectiveness of current controls
- **Output:**

Likelihood rating of High, Medium or Low



## Risk Assessment Methodology

---

### ○ Step 6: Impact Analysis

- **Input:**
  - System mission
  - System and data criticality
  - System and data sensitivity
- **Analysis:**

Adverse impact described in terms of loss or degradation of integrity, confidentiality, availability
- **Output:**

Impact Rating of High, Medium or Low

## Risk Assessment Methodology

### ○ Step 7: Risk Determination

- **Input:**

- Likelihood of threat
- Magnitude of risk
- Adequacy of planned or current controls

- **Output:**

- Risk Level Matrix (Risk Level = Threat Likelihood x Threat Impact)
- Risk Scale and Necessary Actions

## Risk-Level Matrix

Threat Likelihood	Impact		
	<i>Low</i> (10)	<i>Medium</i> (50)	<i>High</i> (100)
<i>High</i> (1.0)	<i>Low</i> $10 \times 1.0 =$ <b>10</b>	<i>Medium</i> $50 \times 1.0 =$ <b>50</b>	<i>High</i> $100 \times 1.0 =$ <b>100</b>
<i>Medium</i> (0.5)	<i>Low</i> $10 \times 0.5 =$ <b>5</b>	<i>Medium</i> $50 \times 0.5 =$ <b>25</b>	<i>Medium</i> $100 \times 0.5 =$ <b>50</b>
<i>Low</i> (0.1)	<i>Low</i> $10 \times 0.1 =$ <b>1</b>	<i>Low</i> $50 \times 0.1 =$ <b>5</b>	<i>Low</i> $100 \times 0.1 =$ <b>10</b>

## Risk Scale & Necessary Actions

---

Risk Level	Risk Description and Necessary Actions
High	<ul style="list-style-type: none"><li>○ Strong need for corrective measures</li><li>○ Corrective action plan must be put in place as soon as possible</li></ul>
Medium	<ul style="list-style-type: none"><li>○ Corrective actions are needed</li><li>○ Plan must be developed within a reasonable period of time</li></ul>
Low	<ul style="list-style-type: none"><li>○ Determine whether corrective actions are still required or decide to accept the risk</li></ul>

## Risk Assessment Methodology

---

- Step 8: Control Recommendations
  - Factors to consider
    - Effectiveness of recommended option
    - Legislation and regulation
    - Organizational policy
    - Operational impact
    - Safety and reliability
  - **Output:**  
Recommended controls and alternative solutions to mitigate risk



## Risk Assessment Methodology

---

- Step 9: Results Documentation

- **Output:**

- **Risk Assessment Report**

- Presented to senior management and mission owners
      - Describes threats & vulnerabilities, measures risk and provides recommendations on controls to implement
      - Purpose: Assist decision-makers in making decisions on policy, procedural, budget and system operational and management changes