Let's look at SP800-30 Risk Management Guide for Information Technology Systems (September 2012)
- What follows are the NIST SP800-30 slides, which are available from the web

Another NIST SP is: Managing Risk from Information Systems: An Organizational Perspective
- PS800-39 (March 2011)

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

- 1st 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
<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Threat-Source</th>
<th>Threat Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminated employee ID’s are not removed from the system</td>
<td>Terminated employees</td>
<td>Dialing into the company’s network and accessing proprietary info</td>
</tr>
<tr>
<td>Water sprinklers used for fire suppression and no protective coverings in place</td>
<td>Fire; negligent persons</td>
<td>Water sprinklers being turned on</td>
</tr>
<tr>
<td>Vendor has identified security flaws in system and patches have not been applied</td>
<td>Unauthorized users (e.g. terminated employees, hackers)</td>
<td>Obtaining unauthorized access to sensitive files based on known vulnerabilities</td>
</tr>
</tbody>
</table>
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 ($\text{Risk Level} = \text{Threat Likelihood} \times \text{Threat Impact}$)
    - Risk Scale and Necessary Actions
# Risk-Level Matrix

<table>
<thead>
<tr>
<th>Threat Likelihood</th>
<th>Low (10)</th>
<th>Medium (50)</th>
<th>High (100)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong> (1.0)</td>
<td>Low 10 X 1.0 = <strong>10</strong></td>
<td>Medium 50 X 1.0 = <strong>50</strong></td>
<td>High 100 X 1.0 = <strong>100</strong></td>
</tr>
<tr>
<td><strong>Medium</strong> (0.5)</td>
<td>Low 10 X 0.5 = <strong>5</strong></td>
<td>Medium 50 X 0.5 = <strong>25</strong></td>
<td>Medium 100 X 0.5 = <strong>50</strong></td>
</tr>
<tr>
<td><strong>Low</strong> (0.1)</td>
<td>Low 10 X 0.1 = <strong>1</strong></td>
<td>Low 50 X 0.1 = <strong>5</strong></td>
<td>Low 100 X 0.1 = <strong>10</strong></td>
</tr>
</tbody>
</table>
## Risk Scale & Necessary Actions

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Risk Description and Necessary Actions</th>
</tr>
</thead>
</table>
| **High**   | ◦ Strong need for corrective measures  
             ◦ Corrective action plan must be put in place as soon as possible |
| **Medium** | ◦ Corrective actions are needed        
             ◦ Plan must be developed within a reasonable period of time |
| **Low**    | ◦ Determine whether corrective actions are still required or decide to accept the risk |
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