Risk Assessment Guidelines

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545may_060106_cd44

Information System Security
Risk Assessment Guidelines
for System Owners and Information System Security Officers

Risk assessment is the first process in risk management. USAID uses risk assessment to determine the extent of the potential threat and the risk associated with its information systems. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

The risk assessment process consists of a number of steps. The method described in the following sections can be applied to a single system or multiple interrelated systems. The first step is to identify the purpose and scope of the risk assessment to be performed.

1. Purpose and Scope

Determine the risk assessment purpose and scope. This establishes the extent of the assessment to be performed. Identify the system components, field site locations (if any), and any other details about the information system to be considered.

Once you have identified the purpose and scope, the next step is to identify the risk assessment approach.

2. Risk Assessment Approach

Determine the approach used to conduct the risk assessment, including:

- The participants (e.g., risk assessment team members)
- The technique used to gather information (e.g., the use of tools, questionnaires)
- The development and description of risk scale and risk-level matrix.

To measure risk, you must develop a risk-level matrix. The matrix uses threat impact and threat likelihood to obtain a risk level. Generally a three by three matrix is used, with a threat impact of high, medium, and low, and a threat likelihood of high, medium, and low. Likelihood and impact values are assigned a numerical rating. The combination of likelihood x impact produces a risk-level value, as shown below:

		Threat Impact		
		Low (10)	**Medium (50)**	**High (100)**
Threat Likelihood	**High (1.0)**	L (10)	M (50)	H (100)
	Medium (0.5)	L (5)	M (25)	M (50)
	Low (0.1)	L (1)	L (5)	L (10)
High = >50-100, Medium = >10-50, Low = 1-10				

The above table is a simple matrix that shows how to determine the risk level based upon the threat impact and the threat likelihood.

Example: For a High likelihood (1.0) and Medium impact (50) threat, the risk level is 1 x 50 = 50 = Medium risk.

If necessary, a four by four or five by five matrix may be used, that includes the values “very high” and/or “very low” in the risk scale. Once you have established the risk assessment approach and risk matrix, the next step is system characterization.

3. System Characterization

Identify the specific system components. System components should include:

- Hardware (server, router, switch),
- Software (e.g., application, operating system, protocol),
- System interfaces (e.g., communication link),
- Data, and
- Users.

Provide a connectivity diagram or system flowchart to define the scope of the risk assessment effort. When you have identified the system, the next step is to list the potential system threats.

4. Threat Identification

A threat is an individual or activity with the potential to cause harm to the system. A threat-source is the intent or situation, and method that may trigger the threat. Compile and list the potential threat-sources that apply to the system assessed.

The following table lists some common threat-sources:

Natural	Human	Environmental
Flood	Hacker	Power failure
Earthquake	Computer criminal	Pollution
Electrical storm	Terrorist	Chemicals
Avalanche	Industrial espionage	Leakage
Tornado	Insiders (employees)	Electrical fire

This table lists common threat-sources by natural, human and environmental categories.

After you have identified the potential threats, the next step is to identify system vulnerabilities.

5. Vulnerability Identification

A vulnerability is a weakness in the system security that could be exploited and result in a security breach. The analysis of the threat to an information system must include the vulnerabilities associated with the system. This information can then be expressed as a threat-vulnerability pair.

The following table lists some examples of threat-vulnerability pairs:

Threat-Source	Vulnerability	Threat Action
Terminated employees.	Terminated employees' system identifiers (ID) are not removed from the system.	Dialing into the company's network and accessing company proprietary data.
Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists).	Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server.	Using telnet to XYZ server and browsing system files with the *guest* ID.
Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists).	The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system.	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities.
Fire, negligent persons.	Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place.	Water sprinklers being turned on in the data center.

This table lists threats, vulnerability, and threat actions.

When you have gathered all the threat and vulnerability information, the risk assessment can begin.

6. Risk Assessment

During the risk assessment, the assessment team evaluates the threat-vulnerability pairs identified for the system. The assessment team evaluates the threat-vulnerability pairs in terms of likelihood and impact. A risk-level value is assigned for the pair using the established risk-level matrix. This evaluation will result in the risk level for the system.

The assessment team observations should be summarized in a table. Each observation must include the following information:

- A brief description of observation (e.g., Observation 1: User system passwords can be guessed or cracked).
- The threat-source and vulnerability pair.
- Existing mitigating security controls.
- Threat likelihood evaluation (e.g., High, Medium, or Low).
- Threat impact evaluation (e.g., High, Medium, or Low).
- Risk rating based on the established risk-level matrix (e.g., High, Medium, or Low).

- Recommended controls or alternative options for reducing the risk.

The assessment results should be ordered by risk level, i.e. high, medium, and then low risk items. Within the risk level, the items with the greatest impact should be listed first. An example of a risk assessment summary is shown below. For a template see **Risk Assessment Results Template**.

[Note: this document is only available on the USAID intranet. Please contact **ads@usaid.gov** if you need a copy.]

Observation Description	Threat Source	Vulnerability	Existing Controls	Likeli-hood	Impact	Risk Level	Recommended Controls
Unauthorized users can access XYZ server via telnet and browse sensitive company files with *guest* ID.	Unauthorized users (e.g., hackers)	Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server.	None.	H (1)	H (100)	H (100)	Disable the *guest* ID.
Unauthorized users can access sensitive system files based on known system vulnerabilities.	Unauthorized users (e.g., hackers)	The vendor has identified flaws in the security design of the system; however new patches have not been applied to the system.	Firewall in place to prevent unauthorized access.	M (0.5)	H (100)	M (50)	Install patches on the system when they arrive from the vendor.
Terminated employees can access system.	Terminated employees	Terminated employees system identifiers (IDs) are not removed from the system within 30 days.	Account will automatically lockout after 90 days.	L (0.1)	H (100)	L (10)	Terminated employees IDs removed from the system within 3 business days.

This table is a risk assessment summary that lists determined characteristics of each identified risk.

Once you have completed the assessment, document the results in a report. Management will use the report to make decisions on policy, system, and management changes. Management can then allocate the necessary resources to mitigate risks to the information system.

References

NIST SP 800-30, **Risk Management Guide for Information Technology Systems**, July 2002.