Performing Risk Assessment

A detailed Plan

Prepare for RA

- Before progressing with the RA, you need to complete three preliminary actions.
  - Define the assessment.
  - Review previous findings.
  - Identifying the Management Structure

Prepare for RA

- Define the assessment.
  - Will you assess a SYSTEM or a PROCESS
  - As there are always change, Describe the system/process as its current situation
  - focus on two primary areas:

Operational characteristics

- Operational characteristics define how the system operates in your environment.
- You need to ask the following simple questions to the relevant entities during this step:
  - • Do you have current diagrams that show all of the current systems?
  - • Do you have documentation of the current configuration?

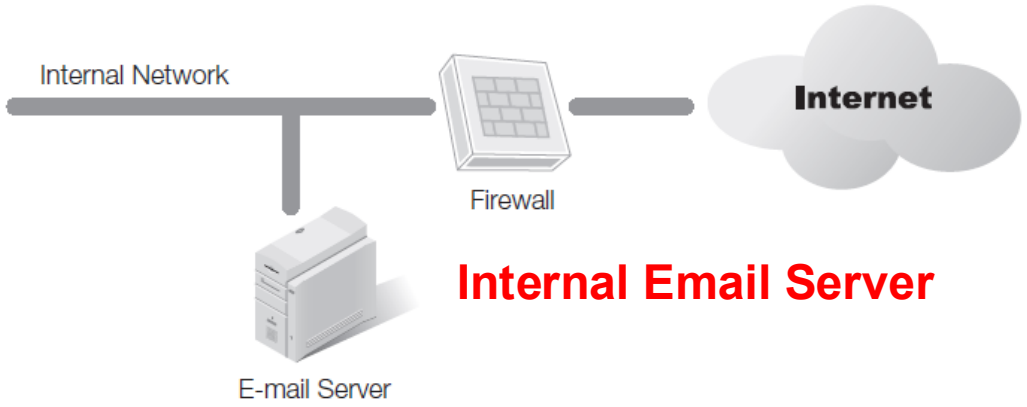
Mission of the System

Short sentence describes what the system does.

- No much details.
- Compared to operational characteristics, the mission is easy to define.

Prepare for RA

- Example of Operational Characteristics



Internal Email Server

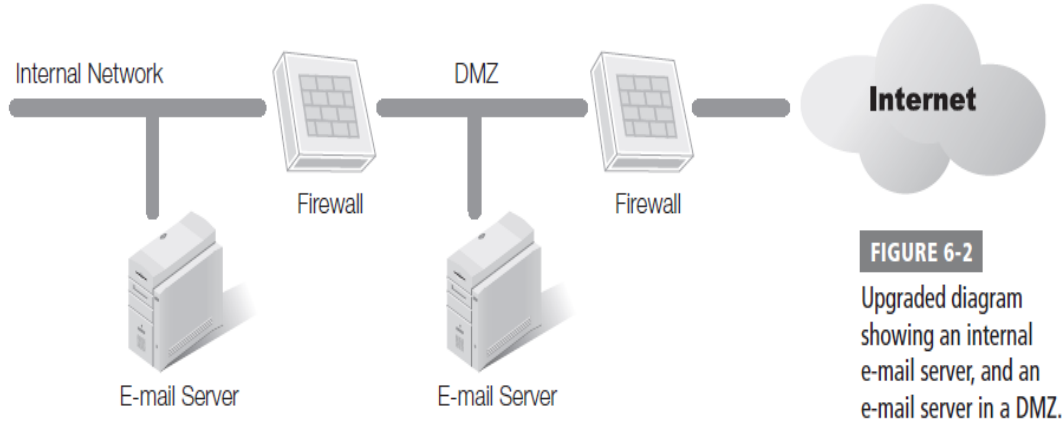


FIGURE 6-2
Upgraded diagram showing an internal e-mail server, and an e-mail server in a DMZ.

Two email servers (internal +DMZ)

- Example of System mission

The e-mail server provides all e-mail services for the network. This includes the following functions:

- Routing e-mail between internal clients
- Accepting e-mail from external e-mail servers and routing to internal client
- Accepting e-mail from internal clients and routing to external e-mail servers
- Scanning all e-mail attachments and removing malware
- Scanning all e-mail for spam and stripping out confirmed spam

Prepare for RA

- Review Previous Findings
  - Start from where the others end
  - These reports can contain a lot of valuable information to make your job easier (assets, threats, vulnerabilities, recommendations, controls).
  - Pay more attention to:
    - Recommendations—Previous recommendations give insight into several issues.
    - Current status of accepted recommendations—
      - Measure the effectiveness of recommendation in place.
      - Find justification of recommendation not in place.
    - Unapproved recommendations—The recommendations that were not approved can also give some insight into the business.
      - level of residual risk.
      - Receptiveness of organization to the control.

Prepare for RA

- Identifying the Management Structure
  - refers to how responsibilities are assigned. When you define the scope of the RA,
    - it's helpful to keep the scope within the ownership of a single entity.
  - Is IT controlled by one entity or multiple entities?
    - Network infrastructure
    - User and computer management
    - E-mail servers
    - Web servers
    - Database servers
    - Configuration and change management – systematic & consistent with proper documentation

RA plan (steps to do)

- RA is not a one day project, it is a continuous process.
- It takes time and planning.
- a risk assessment involves the following steps:
  1. Identify assets and activities to address.
  2. Identify and evaluate relevant threats.
  3. Identify and evaluate relevant vulnerabilities.
  4. Identify and evaluate relevant countermeasures.
  5. Assess threats, vulnerabilities, and exploits.
  6. Evaluate risks.
  7. Develop recommendations to mitigate risks.
  8. Present recommendations to management.

Identify assets and activities to address.

- **Asset valuation**
  - It is important that you evaluate only assets that are within the boundary of the RA.
  - Scope creep occurs when you start evaluating assets outside the scope of the RA.
    - This results in wasted time and wasted resources.

Identify assets and activities to address.

- **Asset valuation**
  - When considering the value of an asset, you can look at it from different perspectives:
    - **Replacement value**—This is the cost to purchase a new asset in its place.
      - For example, if a laptop fails or is stolen, the price to purchase a new laptop with similar hardware and software may be $1,500.
    - **Recovery value**—This is the cost to get the asset operational after a failure.
      - For example, if the hard drive on a server fails, you wouldn't replace the entire server. Instead, you'd replace the hard drive and take steps to recover the system. This may require you to reinstall the operating system and restore data from a backup.
      - You would also consider the time needed to perform the repair. For example, if a repair requires two hours, the system is not available for two hours. If it's a Web server generating $10,000 an hour in revenue, you would include $20,000 as part of the recovery value.

Identify assets and activities to address.

- There are several elements to consider when determining the value of different assets.
  - System access and system availability: available 24/7 or during office hours.
  - System functions: is the function automated or it requires an interactions.
  - Hardware assets & Software assets
  - Personnel assets: some organization are stable in retaining employee, while others are having high turnover. The second type has a higher cybersecurity issues.
  - Data and information assets: Data classification to know the protection level of each.
  - Facilities and supplies:
    - insurance
    - Redundancy: hot site, cold site, and warm site

Identifying and Evaluating Relevant Threats

- **You can use one of two primary methods to identify threats. They are:**
  - **Review historical data: attacks, natural effects, equipment failure, Accidents**
  - **Threat Modeling**

Identifying and Evaluating Relevant Vulnerabilities

- Vulnerability Assessments
  - Information gathering and capturing:
    - Identify the used IP addresses: PING
    - Identify the domain names: WHOIS
    - Identify the running OS: fingerprint attack
    - Identify the weak password: Password Cracking
    - Identify the open ports: port scan
    - Capture data: NMAP, NESSUS, SATAN, SAINT
- Exploit Assessment:
  - Penetration Testing

Identifying and Evaluating Countermeasures

- When identifying and evaluating the countermeasures, you should consider:
  - In-place controls—The controls that are currently installed in the operational system.
  - Planned controls—The controls that have a specified implementation date.
  - Control categories—Controls fall into three primary categories: administrative controls, technical controls, and physical controls.
- When reviewing all of the controls, you should consider the purpose.

CONTROL CLASS	CONTROL FAMILIES
Management	Security and assessment and authorization Planning Risk assessment System and services acquisition Program management
Technical	Access control Audit and accountability Identification and authentication System and communications protection
Operational	Awareness and training Configuration management Contingency planning Incident response Maintenance Media protection Physical and environment protection Personnel security System and information integrity

Develop Mitigating Recommendations

- Threat/vulnerability pairs
- Estimate of cost and time to implement
- Estimate of operational impact
- Cost-benefit analysis

Present Risk Assessment Results

- Phase one
  - The list of ranked risks submitted to Top management for approval.
- Phase TWO
  - POAM: Plan Of Actions and Milestones
    - How to implement the approved items according the given budget and time.

Best Practices for Performing Risk Assessments

- Ensure systems are fully described.
- Review past audits
- Review past risk assessments
- Match the RA to the management structure (ownership & Responsibilities) – Don't cross the management lines.
- Identify assets within the RA boundaries
- Identify and evaluate relevant threats
- Identify and evaluate relevant vulnerabilities
- Identify and evaluate countermeasures
- Track the results: POAM