Risk Frameworks

Objectives

- Understand what frameworks are and how they are used
- Discuss how you need tools to support you throughout the process
- Understand how to get buy in from everyone who is involved

What is Risk Management Framework?

- A risk management framework is a workflow and processes based approach to managing both
  - Operational Risk
  - Organizational Risk
- Integrates security and risk management activities throughout the system lifecycle
- Key step in providing an effective information security program

NIST 800-37

- Entitled Guide for Applying the Risk Management Framework to Federal Information Systems
- Provides a framework for ongoing, near real-time risk management for system lifecycles
- Provides leadership insight into making cost-effective, risk-based decisions

Steps

- Categorize
- Select
- Implement
- Assess
- Authorize
- Monitor

Step 1 - Categorize

- Summary: What is the system and how is it used? How important is it?
- Who’s responsible: Information System Owner
- How it is used: Identifies the criticality of the system.
- Examples:
    - A credit card payment server
    - A credit card terminal
    - A server with photos on it

Step 2 – Select

- Summary: Select what kind of security controls will be placed on the system based on the criticality
- Who's responsible: Information Security Office
- How it is used: Based on the criticality of the system, different controls should be selected. You may not have high security controls on everything
- Examples:
  - Determining to put Multifactor authentication on financial systems
  - Identifying antivirus requirement on employee workstations

Step 3 - Implement

- Summary: Implementing the actual controls you selected
- Who’s responsible: Information System Owner
- How it is used: Very simple – do the work you said you were going to do to meet the security control
- Examples:
  - Deploying security controls such as multifactor authentication and antivirus on specific systems

Step 4 - Assess

- Summary: Development of processes used to ensure information system security controls are in place
- Who’s responsible: Auditing/Information Security Office
- How it is used: This can be a time consuming process of assessing if the security controls are actually working as intended.
- Examples:
  - Does multifactor authentication work correctly?
  - Does antivirus actually protect against the threats out there?
  - Do we have any additional threats that were not identified?

Step 5 - Authorize

- Summary: If risk is identified, how is it mitigated or do we accept the risk?
- Who’s responsible: Auditing/Information Security Office
- How it is used: If the assessment process has identified residual risk or if security controls are not effective, risk must be accepted or mitigated
- Examples:
  - Certain antivirus cannot be placed on point of sale terminals
  - Multifactor authentication would be too cumbersome for some users

Step 6 - Monitor

- Summary: Continually monitor the information system and security controls to determine their effectiveness
- Who's responsible:
- How it is used: Document changes to environment, conduct analysis of security controls and monitor their status
- Examples:
  - Logging
  - System Monitoring

Complete Picture

- A complete framework must work for your environment
- You must have buy-in from all parties
  - Information System Owners
  - Information Security Office
  - Senior management