Management of Information Security, 4th Edition

Chapter 7

Security Management Practices

Objectives

- List the elements of key information security management practices
- Describe the key components of a security metrics program
- Identify suitable strategies for the implementation of a security metrics program
- Discuss the emerging trends in the certification and accreditation (C&A) of information technology (IT) systems

Benchmarking

- **Benchmarking** - creating a security blueprint
  - Can help determine which controls should be considered
  - Cannot determine how those controls should be implemented in your organization
- In InfoSec, two categories of benchmarks are used
  - Standards of due care and due diligence
  - Recommended practices (also known as “best security practices”)

Standards of Due Care/Due Diligence

- **Standard of due care**: a means of assessing planned actions by considering what would be reasonable if done by another similar and prudent organization in similar circumstances
  - Sometimes known as simply “due care”
- **Due diligence**: a requirement that implemented standards continue to be applied to provide the required level of protection
  - Also known as a “standard of due diligence”
- Failure to establish and maintain these standards can expose an organization to legal liability

Recommended Security Practices

- **Recommended business practices**: security efforts that seek to provide a superior level of performance in the protection of information
  - Security efforts that are considered among the best in the industry are termed best security practices (BSPs)
- The federal government maintains a Web site that allows agencies to share recommended security practices
  - Was begun as part of the Federal Agency Security Project (FASP)

Recommended Security Practices (continued)

- FASP was established by the Federal Chief Information Officer (CIO) Council
- The FASP site contains examples of many agencies' policies, procedures, and practices
- Many of the BSPs found on the FASP Web site can be applied to InfoSec practices in both the public and private sectors
- Table 7-1 starting on page 250 of the textbook shows Federal agency BSPs

Selecting Recommended Practices Part 1

- Industries regulated by laws and standards and are subject to government or industry oversight:
  - Are required to meet the regulatory and industry guidelines in their security practices
- For other organizations:
  - Government and industry guidelines can serve as an excellent source about what is required to control InfoSec risks
- Standards of performance can inform the selection of recommended practices

Selecting Recommended Practices Part 2

- Consider the following questions when selecting recommended practices:
  - Does your organization resemble the target organization of the recommended practice?
  - Are you in a similar industry as the target?
  - Do you face similar challenges?
  - Is your organizational structure similar to the target?
  - Can your organization expend resources at the level required by the recommended practice?
  - Is your threat environment similar?

Selecting Recommended Practices Part 3

- Sources of information on recommended practices:
  - National Institute for Standards and Technology (NIST) practices
  - Carnegie Mellon University's Computer Emergency Response Team Coordination Center (CERT?CC) Web site
- Goal:
  - To obtain a methodology for creating a framework that meets your situation

Limitations to Benchmarking and Recommended Practices

- Biggest barrier to benchmarking in InfoSec:
  - Many organizations do not share results with other organizations
  - Valuable lessons are not recorded, disseminated, and evaluated
- Some security administrators are joining professional associations and societies and are sharing stories and lessons they've learned
- Other groups publish versions of attacks, in security journals, while leaving out the identifying details

Limitations to Benchmarking and Recommended Practices (continued)

- Another barrier to benchmarking: no two organizations are identical
  - The number and types of variables that affect security are likely to differ between any two organizations
- Third problem with benchmarking: recommended practices are a moving target
  - Security programs must keep abreast of new threats as well as the methods, techniques, policies, guidelines, educational and training approaches to combat them

Baselining

- **Baseline**: an assessment of the performance of some action or process measured against a prior assessment or an internal goal
- **Baselining**: the process of measuring against an established internal value or standard
- In InfoSec, baseline measurements of security activities and events:
  - Are used to provide a comparison of the organization's current security performance against prior performance

Support for Benchmarks and Baselines Part 1

- By baselining and seeking to use benchmarks:
  - You can piece together the desired outcome of the security process
- Then, work backward to achieve an effective design of a methodology
- NIST publications written to support baselining:
  - SP 800-27, Rev. A, SP 800-53, Rev. 4, SP 800-53A, Rev. 1
  - These documents are available at *csrc.nist.gov* under the Special Publications link

Support for Benchmarks and Baselines Part 2

- CERT (*www.cert.org*) - source for recommended practices
  - Provides links to security practices and implementations
- Many organizations sponsor seminars and classes on recommended practices for implementing security
  - Information Systems Audit and Control Association (*www.isaca.org*) hosts seminars on a regular basis

Support for Benchmarks and Baselines Part 3

- The Gartner Group has published 12 questions to be used as a self-assessment for recommended security policies
  - Questions are organized into three categories - people, processes, and technology
- **People**
  - Do you perform background checks on all employees with access to sensitive data, areas, or access point?
  - Would the typical employee recognize a security issue?

Support for Benchmarks and Baselines Part 4

- **People** (cont'd)
  - Would the typical employee choose to report it?
  - Would the typical employee know how to report it to the right people?
- **Processes**
  - Are enterprise security policies updated on at least an annual basis, employees educated on changes, and policies consistently enforced?
  - Does your enterprise follow a patch/update management and evaluation process to prioritize and mediate new security vulnerabilities?

Support for Benchmarks and Baselines Part 5

- **Processes** (cont'd)
  - Are user accounts of former employees immediately removed on termination?
  - Are security group representatives involved in all stages of the project life cycle for new projects?
- **Technology**
  - Is every possible network route to the Internet protected by a properly configured firewall?
  - Is sensitive data on laptops and remote systems secured with functional encryption practices?

Support for Benchmarks and Baselines

- **Technology** (cont'd)
  - Are your information assets and the systems they use regularly assessed for security exposures using a vulnerability analysis methodology?
  - Are systems and network regularly reviewed for malicious software and telltales from prior attacks?
- The Payment Card Industry Security Standards Council published Data Security Standards (PCI DSS)
  - Considered recommended or best practices for organizations using payment cards

Performance Measurement in InfoSec Management

- Benefits and performance of InfoSec are measurable
  - Doing so requires the design and ongoing use of an InfoSec performance management program based on effective performance metrics

InfoSec Performance Management Part 1

- **InfoSec performance management**: the process of designing, implementing, and managing the use of the collected data elements
  - To determine the effectiveness of the overall security program
- **Performance measurements**: the data points or the trends computed from such measurements that may indicate the effectiveness of security countermeasures or controls
  - Some are technical and some are managerial

InfoSec Performance Management Part 2

- Organizations use three types of measurements:
  - Those that determine the effectiveness of the execution of the InfoSec policy
  - Those that determine the effectiveness and/or efficiency of the delivery of InfoSec services
  - Those that assess the impact of an incident or other security event on the organization or its mission
- Organizations must document that they are taking effective steps to control risk
  - In order to document due diligence

InfoSec Performance Management Part 3

- According to NIST, the following factors must be considered during development and implementation of an InfoSec performance management program:
  - Measurements must yield quantifiable information (percentages, averages, and numbers)
  - Data that supports the measurements needs to be readily obtainable
  - Only repeatable InfoSec processes should be considered for management
  - Measurements must be useful for tracking performance and directing resources

InfoSec Performance Management Part 4

- Also according to NIST's SP 800-55, Rev. 1 - four factors are critical to the success of an InfoSec performance program:
  - *Strong upper-level management support*
  - *Practical InfoSec policies and procedures*
  - *Quantifiable performance measurements*
  - *Results-oriented measurement analysis*

Information Security Metrics

- InfoSec metrics enable organizations to measure the level of effort required to meet the stated objectives of the InfoSec program
- The terms metrics and measurements are sometimes used interchangeably
  - “metrics” is used for more granular, detailed measurements
  - “performance measurements” is used for aggregate, higher-level results
- This text treats the two terms as interchangeable

Information Security Metrics (continued)

- Before designing, collecting, and using measurements, the CISO should be prepared to answer:
  - Why should these measurements be collected?
  - What specific measurements will be collected?
  - How will these measurements be collected?
  - When will these measurements be collected?
  - Who will collect these measurements?
  - Where (at what point in the function's process) will these measurements be collected?

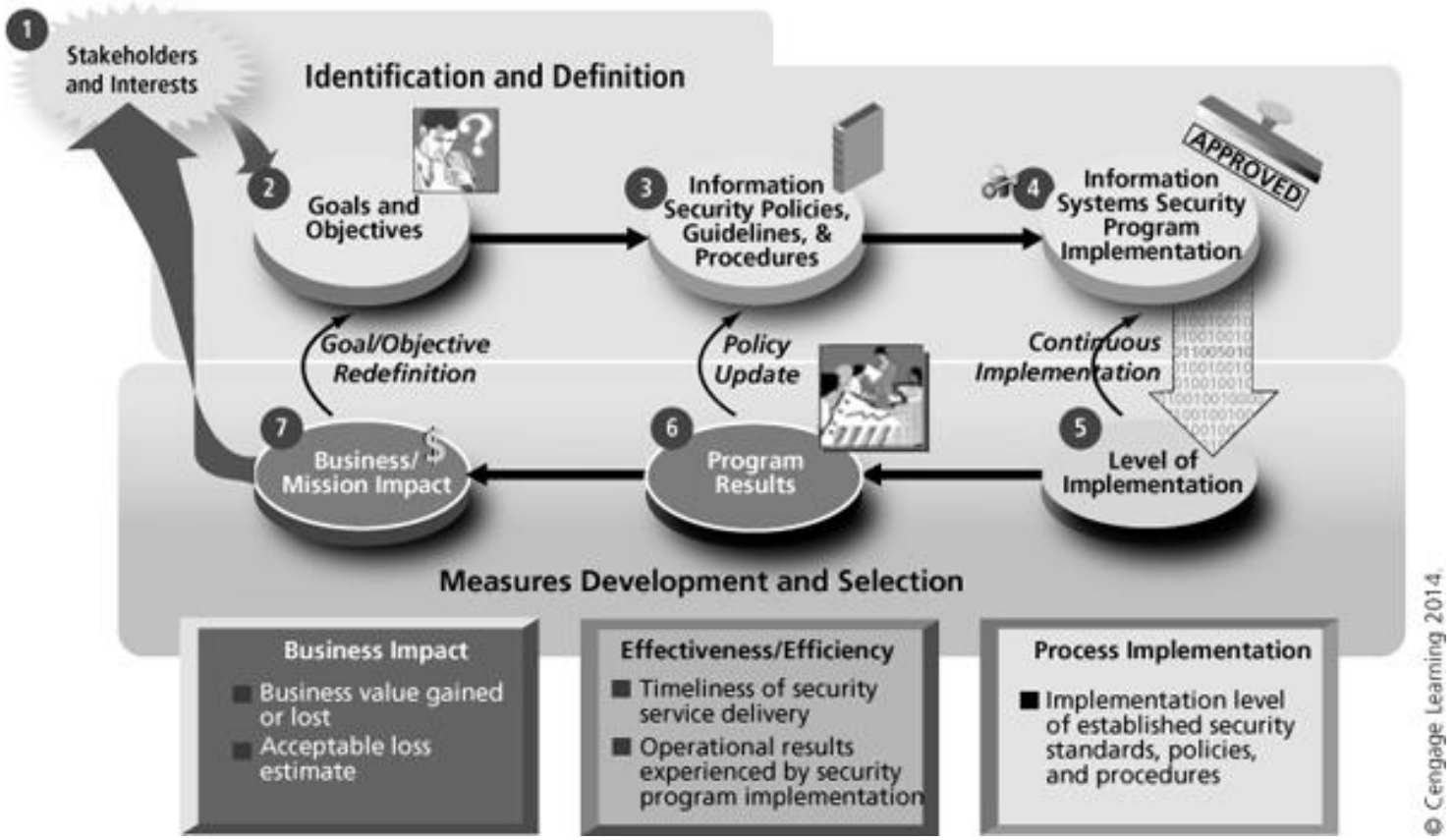
Building the Performance Measurement Program Part 1

- An InfoSec performance measurement program must be able to demonstrate value to the organization
- Benefits of using InfoSec performance measurements:
  - Increasing accountability for InfoSec performance
  - Improving effectiveness of InfoSec activities
  - Demonstrating compliance with laws, rules, and regulations
  - Providing quantifiable inputs for resource allocation decisions

Building the Performance Measurement Program Part 2

- A popular performance measurement approach is NIST's SP 800-55, Rev. 1: Performance Measurement Guide for InfoSec
- It is divided into two major activities:
  - Identification and definition of the current InfoSec program
  - Development and selection of specific measurements to gauge the implementation, effectiveness, efficiency, and impact of the security controls
- It is further divided into seven phases

Figure 7-1 Information security performance measurement development process



Building the Performance Measurement Program Part 3

- Phase 1: identifies relevant stakeholders and their interests in InfoSec measurement
- Phase 2: to identify and document the InfoSec performance goals and objectives that would guide security control implementation for InfoSec
- Phase 3: focuses on organization-specific InfoSec practices
- Phase 4: review of existing measurements
- Phases 5, 6, and 7: involve developing measurements that track process implementation

Specifying InfoSec Measurements

- A critical task in the measurement process:
  - To assess and quantify what will be measured
- Measurements collected from production statistics depend on the number of systems and the number of users of those systems
  - As the number systems/users changes, the effort to maintain the same level of service will vary
- Some organizations track these two values to measure the service
  - Other organizations need more detailed measurement

Collecting InfoSec Measurements Part 1

- Once you know what to measure
  - The how, when, where, and who questions of metrics collection must be addressed
- Designing the collecting process requires thoughtful consideration
- **Measurements Development Approach**
  - Macro-focus measurements: examine the performance of the overall security program
  - Micro-focus measurements: examine the performance of an individual control or group of controls within the InfoSec program

Collecting InfoSec Measurements Part 2

- **Measurement Prioritization and Selection**
  - Important to ensure metrics are prioritized in the same manner as the process that they measure
  - Use a ranking system to achieve this:
    - Low/medium/high ranking scale or a weighted scale
- **Establishing Performance Targets**
  - Performance targets make it possible to define success in the security program
  - Many InfoSec performance measurements targets are represented by a 100 percent target goal

Collecting InfoSec Measurements Part 3

- **Measurements Development Template** - Performance measurements should be documented in a standardized format
  - To ensure the repeatability of the measurement development, customization, collection, and reporting activities
  - A custom template can be developed
  - Instructions for the development and format of such template are provided in Table 7-2 starting on page 262 of the textbook

Collecting InfoSec Measurements Part 4

- **Candidate Measurements**
  - Examples of candidate measurements are provided in Table 7-4 (on the following slide)
  - Additional details on these measurements are provided in “NIST SP 800-55, Rev. 1”

Table 7-4 Examples of possible security performance measurements

- Percentage of the organization's information systems budget devoted to InfoSec
- Percentage of high vulnerabilities mitigated within organizationally defined time periods after discovery
- Percentage space of remote access points used to gain unauthorized access
- Percentage of information systems personnel who have received security training
- Average frequency of audit records review and analysis for inappropriate activity
- Percentage of new systems that have completed C&A prior to their implementation
- Percentage of approved and implemented configuration changes identified in the latest automated baseline configuration
- Percentage of information systems that have conducted annual contingency plan testing
- Percentage of users with access to shared accounts
- Percentage of incidents reported within required time frame per applicable incident category
- Percentage of system components that undergo maintenance in accordance with formal maintenance schedules
- Percentage of media that passes sanitization procedures testing
- Percentage of physical security incidents allowing unauthorized entry into facilities containing information assets
- Percentage of employees who are authorized access to information systems only after they sign an acknowledgement that they have read and understood the appropriate policies
- Percentage of individuals screened before being granted access to organizational information and information systems
- Percentage of vulnerabilities remediated within organizationally specified time frames
- Percentage of system and service acquisition contracts that include security requirements and/or specifications
- Percentage of mobile computers and devices that perform all cryptographic operations using organizationally specified cryptographic modules operating in approved modes of operations
- Percentage of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated.

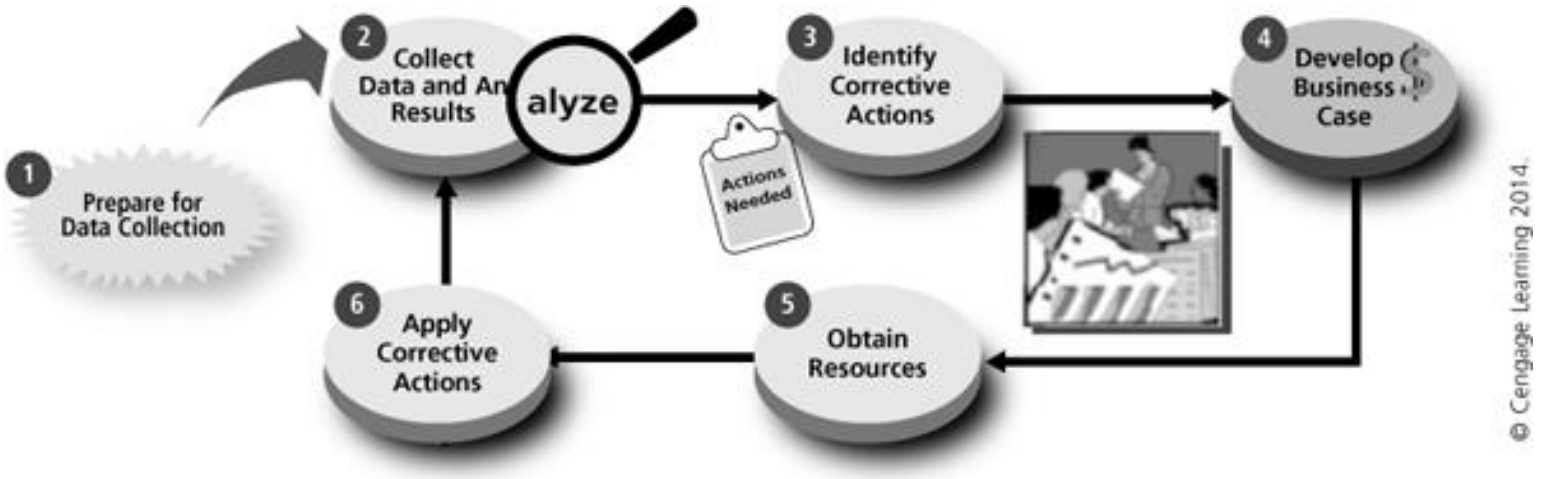
Implementing InfoSec Performance Management

- The process for performance measurement implementation involves six subordinate tasks:
  - *Phase 1* - Prepare for data collection
    - Identify, define, develop, and select InfoSec measures
  - *Phase 2* - Collect data and analyze results
    - Collect, aggregate, and consolidate metric data collection and compare measurements with targets
  - *Phase 3* - Identify corrective actions
    - Develop a plan to serve as the roadmap for closing the gap identified in Phase 2

Implementing InfoSec Performance Management (continued)

- The process for performance measurement implementation involves six subordinate tasks (cont'd):
  - *Phase 4* - Develop the business case
  - *Phase 5* - Obtain resources
    - Address the budgeting cycle for acquiring resources needed to implement remediation actions
  - *Phase 6* - Apply corrective actions

Figure 7-2 Information security measurements program implementation process



Reporting InfoSec Performance Measurements

- When reporting performance measurements:
  - You must make decisions about how to present correlated metrics
    - Whether to use pie, line, scatter, or bar charts
    - Also which colors denote which kinds of results
  - CISO must consider to whom the results should be disseminated and how they should be delivered

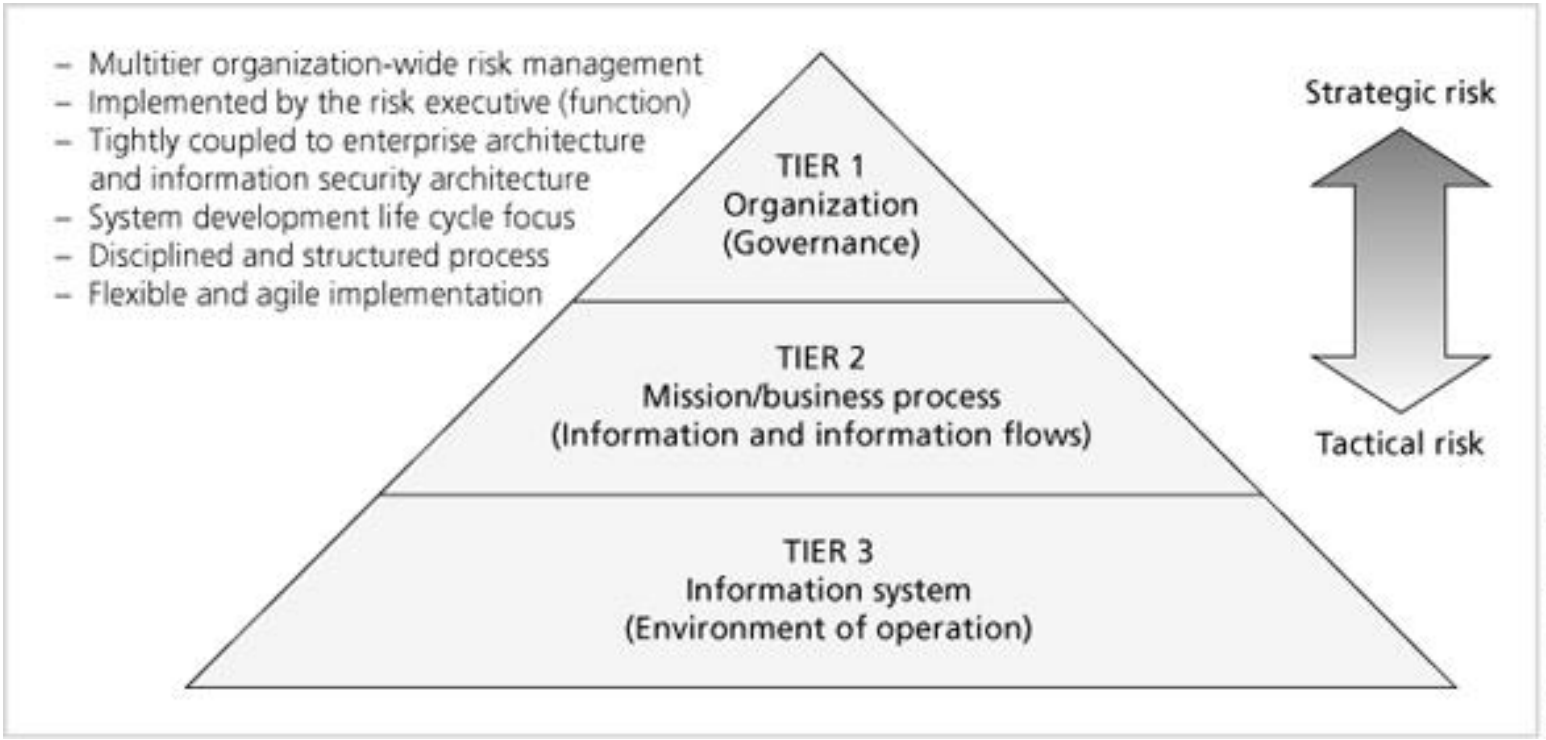
Trends in Certification and Accreditation

- **Accreditation** (in security management) - the authorization of an IT system to process, store, or transmit information
  - Issued by a management official and serves as a means of assuring that systems are of quality
- **Certification** - a comprehensive assessment of both technical and nontechnical protection strategies for a particular system
- Organizations pursue accreditation or certification to gain a competitive advantage or to provide assurance or confidence to their customers

NIST SP 800-37 Rev. 1 Part 1

- With the publication of “NIST SP 800-31, Rev. 1”
  - A common approach to a Risk Management Framework (RMF) for InfoSec practice became the standard for the U.S. government
- NIST follows a three-tiered approach to risk management
  - Most organizations work form the top down, focusing first on aspects affecting the entire organization
  - The most detailed aspects are addressed in tier 3

Figure 7-3 Tiered risk management approach



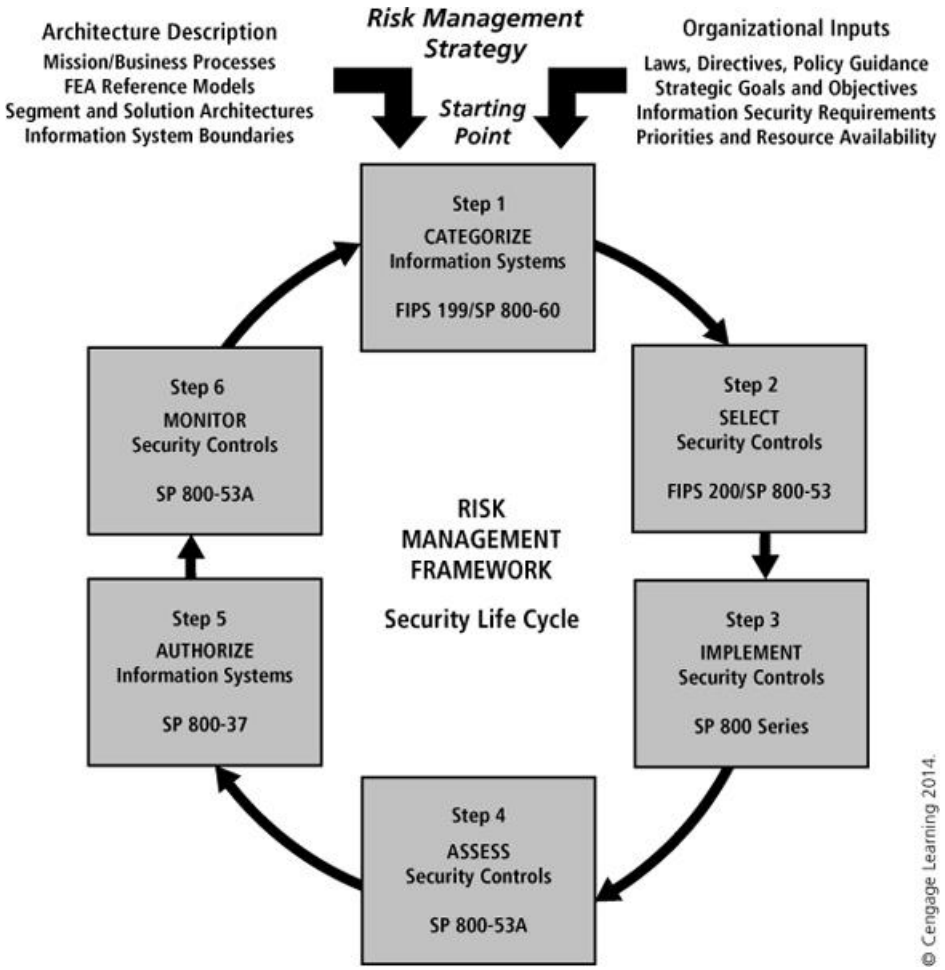
NIST SP 800-37 Rev. 1 Part 2

- RMF applies the multi-tiered approach to a six-step process:
  - 1) Categorize the information system and the information processed, stored, and transmitted by that system
  - 2) Select an initial set of baseline security controls based on the security categorization
  - 3) Implement the security controls and describe how the controls are employed within the information system

NIST SP 800-37 Rev. 1 Part 3

- RMF applies the multi-tiered approach to a six-step process (cont'd):
  - 4) Assess the security controls using appropriate assessment procedures
  - 5) Authorize information system operation based on a determination of the risk to organizational operations and assets
  - 6) Monitor the security controls in the information system on an ongoing basis

Figure 7-4 Risk management framework



NIST SP 800-37 Rev. 1 Part 4

- **Step 4: Assess** - this process involves the development of a plan to assess the security controls in place
- **Step 5: Authorize** - the authorization process involves four tasks:
  - 1) Prepare the plan of action and milestones
  - 2) Assemble the security authorization package and submit the package to the authorizing official
  - 3) Determine the risk to organization operations, assets, individuals, other organizations, or the Nation
  - 4) Determine if the risk is acceptable

NIST SP 800-37 Rev. 1 Part 5

- Accreditation and certification are not permanent
  - Most accreditation and certification processes require reaccreditation or recertification every few years
- Approaches such as the RMF are designed to follow a continuous-improvement method

Summary Part 1

- Benchmarking is a process of following the recommended or existing practices of a similar organization or industry-developed standards
- Organizations may be compelled to adopt a stipulated minimum level of security which is known as a standard of due care
- Security efforts that seek to provide a superior level of performance in the protection of information are called recommended business practices or best practices
- A practice related to benchmarking is baselining which can provide the foundation for internal benchmarking

Summary Part 2

- InfoSec performance management is the process of designing, implementing, and managing the use of the collected data elements called “measurement” to determine the effectiveness of the overall security program
- There are three types of InfoSec performance measures: those that determine the effectiveness of the execution of InfoSec policy, those that determine the effectiveness and/or efficiency of the delivery of InfoSec services, and those that assess the impact of an incident or other security event

Summary Part 3

- One of the critical tasks in the measurement process is to assess and quantify what will be measured and how it is measured
- In security management, accreditation is the authorization of an IT system to process, store, or transmit information
- Certification is the evaluation of the technical and nontechnical security controls of an IT system to establish the extent to which a particular design and implementation meets a set of specified security requirements