CSIT988/CSIT488

Security, Ethics and Professionalism

Week 8: Security Management Practices

Subject Coordinator: Dr Khoa Nguyen

School of Computing and Information Technology

Autumn 2025

Roadmap

- **Security Management Models**
  - Blueprints, Frameworks, Security Models
  - Access Control Models
  - Security Architecture Models
  - Security Management Models

- **Security Management Practices**
  - Benchmarking
  - Performance Measurement in InfoSec management
  - Trends in Certification and Accreditation

Learning Objectives

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

Security Management Practices

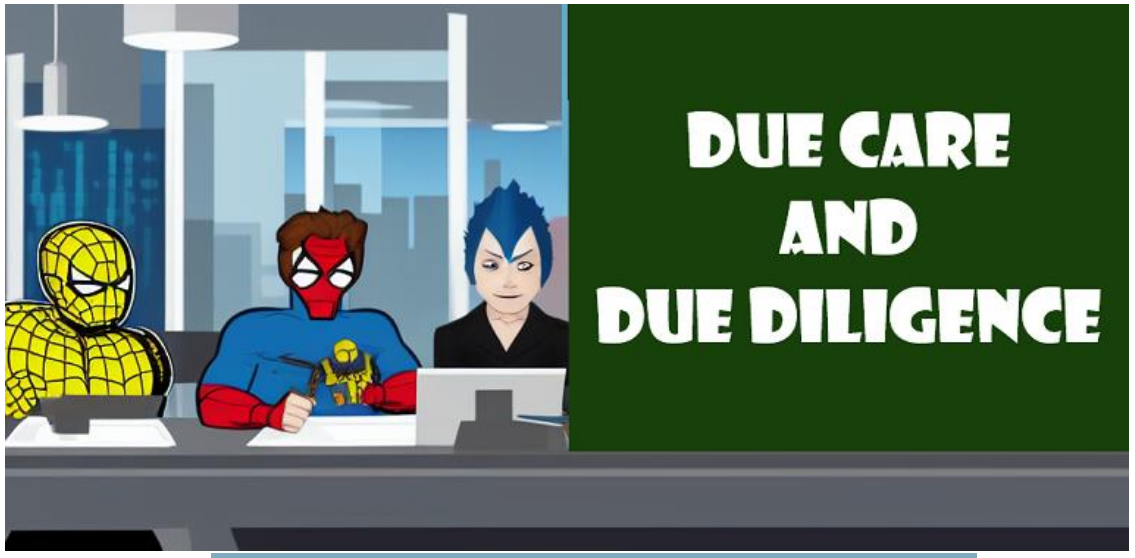
- Value Proposition
  - Organizations strive to deliver the most value with a given level of investment
  - Developing and using sound and repeatable information security management practices makes accomplishing this more likely
- Executives and supervisory groups want assurance that organizations are working toward the value proposition and measuring the quality of management practices.
- This lecture explores various methods of program comparison including benchmarking and compliance measurement.

- To generate a security blueprint
  - ➢ Organizations usually draw from established security models and practices
  - ➢ Another way is to look at the paths taken by organizations similar to the one for which you are developing the plan
- **Benchmarking**
  - ➢ Following the existing practices of a similar organization, or industry-developed standards
  - ➢ Can help to determine which controls should be considered
  - ➢ Cannot determine how those controls should be implemented

Categories of Benchmarks

Categories of benchmarks

- Standards of due care and due diligence
- Best practices
  - Best practices include a sub-category of practices, called the gold standard, that are generally regarded as “the best of the best”



Due Care and Due Diligence

- **Standard of due care**
  - When organizations adopt minimum levels of security for legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances
- **Standard of due diligence**
  - Implementing controls at this minimum standard
  - Requires that an organization ensure that the implemented standards continue to provide the required level of protection
  - Failure to demonstrate due care or due diligence can expose an organization to legal liability, if it can be shown that the organization was negligent in its information protection methods

Recommended Security Practices

Best Practices

- Security efforts that seek to provide a superior level of performance in the protection of information
- Considered among the best in the industry
- Balance the need for information access with the need for adequate protection
- Demonstrate fiscal responsibility
- Companies with best practices may not be the best in every area

Selecting Recommended Practices

- Choosing which recommended practices to implement can pose a challenge for some organizations

  - Industries that are regulated by laws and standards and are subject to government or industry oversight are required to meet the regulatory or industry guidelines in their security practices.

  - For other organizations, government guidelines are excellent sources of information and can inform their selection of best practices

Selecting Recommended Practices (cont'd.)

Considerations for selecting best practices

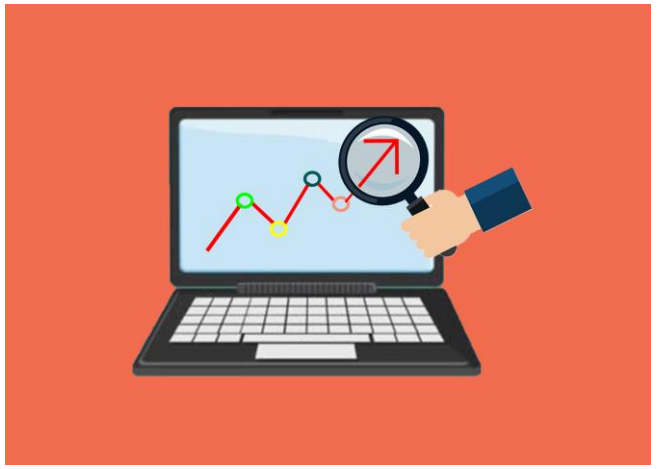
- Does your organization resemble the identified target organization of the best practice?
- Are you in a similar industry as the target?
- Do you face similar challenges as the target?
- Is your organizational structure similar to the target?
- Are the resources you can expend similar to those called for by the best practice?
- Are you in a similar threat environment as the one assumed by the best practice?

Limitations to Benchmarking and Recommended Practices

- **Biggest barrier to benchmarking: Organizations don't talk to each other**
  - ➢ A successful attack is viewed as an organizational failure, and is kept secret, insofar as possible
  - ➢ More and more security administrators are joining professional associations and societies like ISSA and ISACA and sharing their stories and lessons learned
    - ✓ An alternative to this direct dialogue is the publication of lessons learned
- **No two organizations are identical.**
  - ➢ Organizations that offer products or services in the same market may differ dramatically in size, composition, management philosophy, organizational culture, technological infrastructure, and planned expenditures for security.
- **Recommended practices are a moving target.**
  - ➢ Knowing what happened a few years ago does not tell what to do next.

Baselining

- A value or profile of a performance metric against which changes in the performance metric can be usefully compared (e.g., number of attacks per week that an organization experiences)
- Process of measuring against established standards
- Baseline measurements of security activities and events are used to evaluate the organization's future security performance
- Can provide the foundation for internal benchmarking
  - Information gathered for an organization's first risk assessment becomes the baseline for future comparisons



Support for Baselining and Recommended Practices

- Self-assessment for recommended security practices: 12 questions into 3 categories: people, processes and technology, which loosely map to the managerial, operational and technical areas of NIST.

➢ **People:**

✓ Do you perform background checks on all employees with access to sensitive data, areas, or access points?

✓ Would the average employee recognize a security issue?

✓ Would they choose to report it?

✓ Would they know how to report it to the right people?

Support for Baselining and Recommended Practices (cont'd.)

- Self-assessment for recommended security practices (cont'd.)

➢ Processes

- ✓ Are enterprise security policies updated on at least an annual basis, employees educated on changes, and consistently enforced?
- ✓ Does your enterprise follow a patch/update management and evaluation process to prioritize and mediate new security vulnerabilities?
- ✓ Are the 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?

Support for Baselining and Recommended Practices (cont'd.)

- Self-assessment for recommended security practices (cont'd.)

➢ **Technology**

✓ Is every possible route to the Internet protected by a properly configured firewall?

✓ Is sensitive data on laptops and remote systems encrypted?

✓ Do you regularly scan your systems and networks, using a vulnerability analysis tool, for security exposures?

✓ Are malicious software scanning tools deployed on all workstations and servers?

Performance Measurements in Information Security Management

- Costs, benefits and performance of InfoSec are measurable (despite the claim of some CISOs that they are not)
- Measurement requires the design and ongoing use of an InfoSec performance management program based on effective performance metrics

InfoSec Performance Management

- **Information security performance management**

  - The process of designing, implementing and managing the use of collected data elements (called measurements or metrics)
    - ✓ To determine the effectiveness of the overall security program

  - Performance measurements are data points or computed trends that indicate the effectiveness of security countermeasures or controls

InfoSec Performance Management (cont'd.)

- Organizations use three types of measurements
  - Those that determine the effectiveness of the execution of information security policy (most commonly, ISSPs)
  - Those that determine the effectiveness and/or efficiency of the delivery of information security services
  - Those that assess the impact of an incident or other security event on the organization or its mission

InfoSec Performance Management (cont'd.)

- According to NIST SP 800-55 R1, *Performance Measurement Guide for Information Security,* 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 information security processes should be considered for measurement
  - Measurements must be useful for tracking performance and directing resources

InfoSec Performance Management (cont'd.)

- Also, according to "SP 800-55, Rev. 1", four factors are critical to the success of an InfoSec performance program:

  - Strong upper-level management support
  - Practical information security policies and procedures
  - Quantifiable performance measurements
  - Results oriented measurements analysis

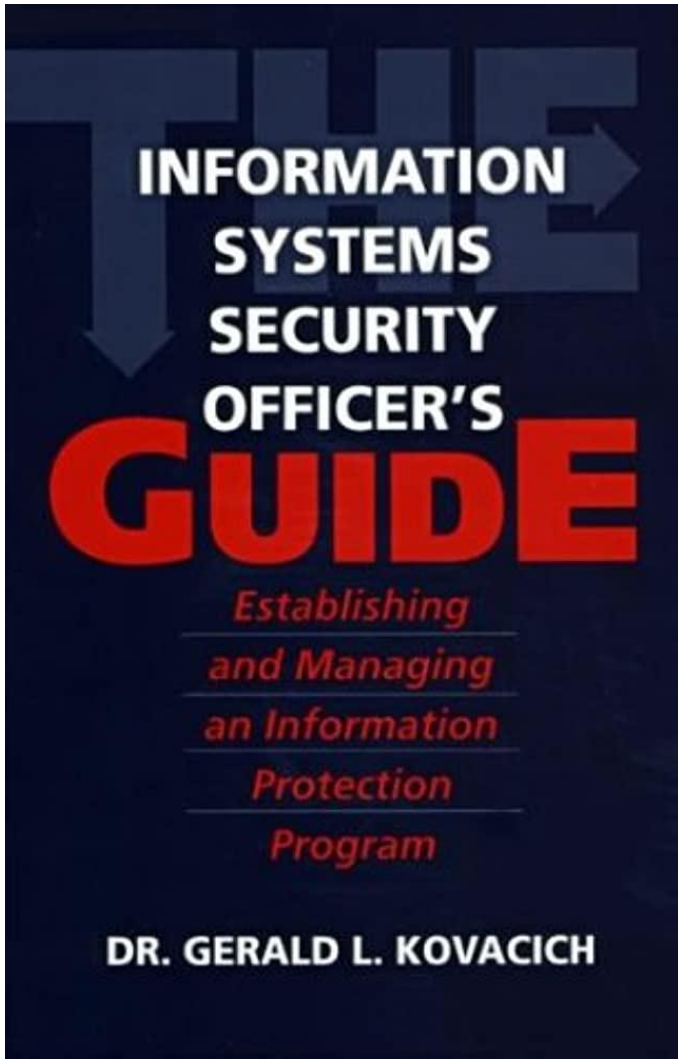
InfoSec Metrics

- **InfoSec metrics**
  - Applying statistical and quantitative approaches of mathematical analysis to the process of measuring the activities and outcomes of the InfoSec program
- The term “metrics” is used for more detailed measurements
- The term “measurements” is used for aggregate, higher-level results
  - The two terms are used interchangeably in some organizations

InfoSec Metrics (cont'd.)

Before beginning the process of designing, collecting, and using measurements, the CISO should be prepared to answer the following questions posed by Gerald Kovacich in *The Information Systems Security Officer's Guide*:

- Why should these statistics be collected?
- What specific statistics will be collected?
- How will these statistics be collected?
- When will these statistics be collected?
- Who will collect these statistics?
- Where (at what point in the function's process) will these statistics be collected?



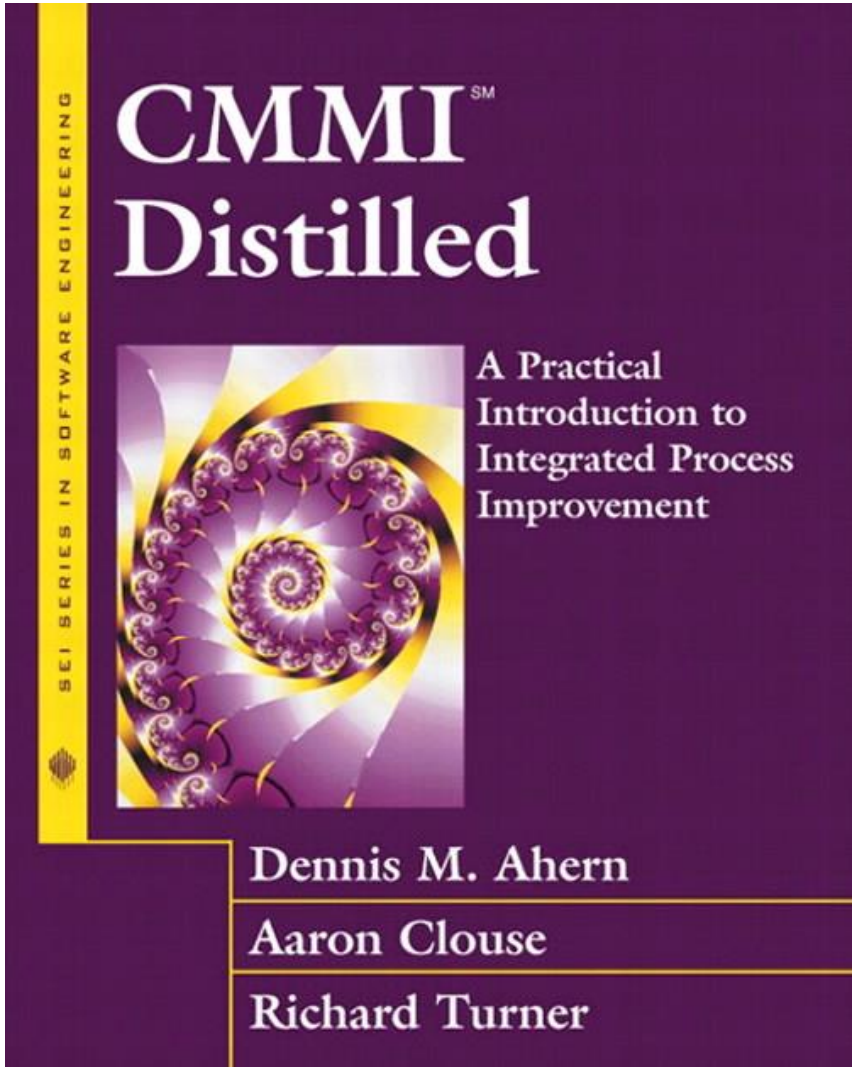
Building the Performance Measurement Program

- An InfoSec measurement program must be able to demonstrate value to the organization.

- According to SP 800-55, Rev. 1, the benefits of using InfoSec performance measurements include:
  - Increasing accountability of InfoSec performance
  - Improving effectiveness of InfoSec activities
  - Demonstrating compliance with laws, rules and regulations
  - Providing quantifiable inputs for resource allocation decisions.

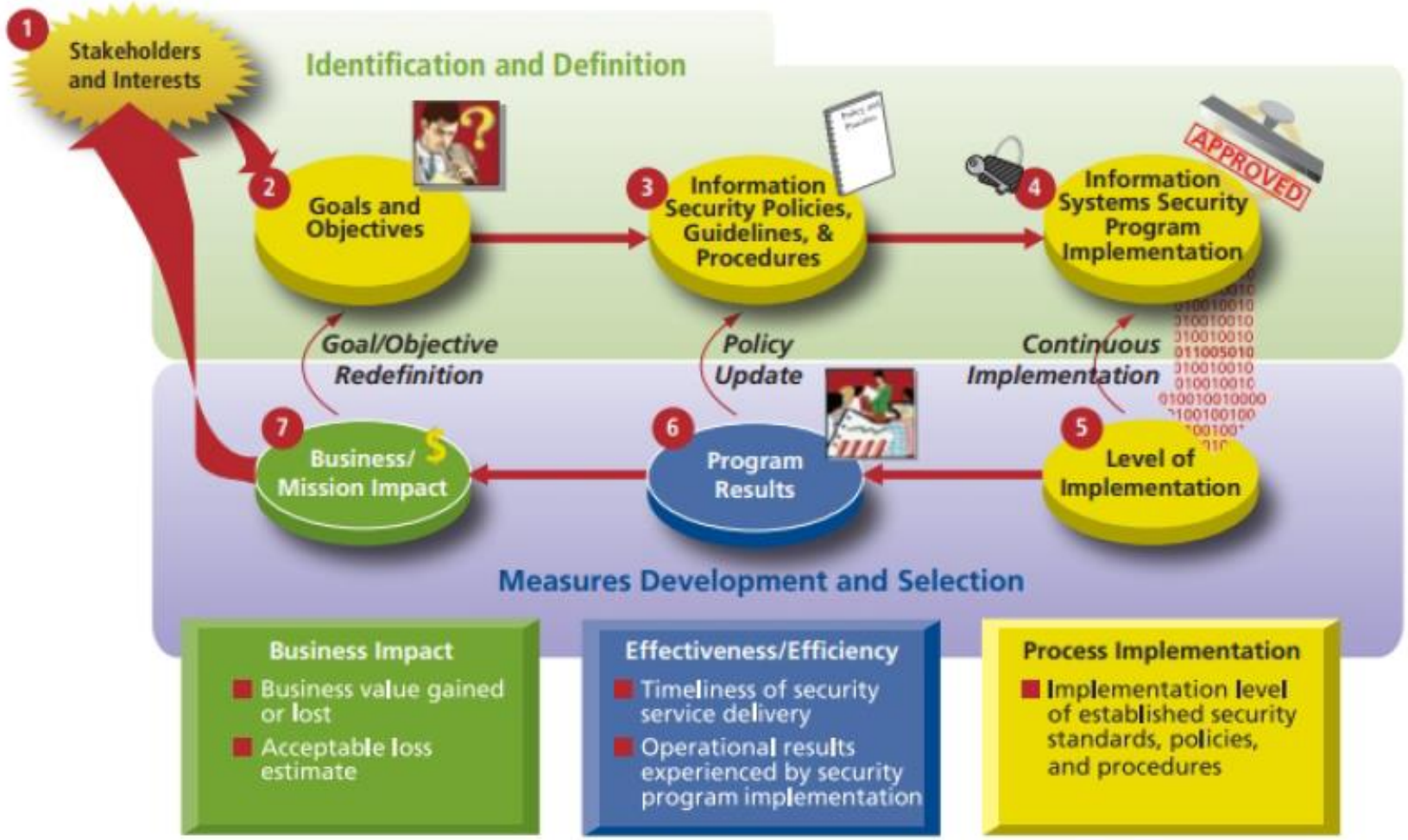
Building the Performance Measurement Program

- **Capability Maturity Model Integration (CMMI)**
  - One of the most popular references that support the development of process improvement and performance measurement is from the publication **CMMI Distilled**
  - Administered by the CMMI Institute (a subsidiary of ISACA), it was developed at CMU.



Another popular approach: NIST SP 800 - 55 Rev. 1. Major activities:

- The 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



Specifying InfoSec Measurements

- One of the critical tasks in the measurement process is to assess and quantify what will be measured. While InfoSec planning and organizing activities may only require time estimates, you must obtain more detailed measurements when assessing the effort spent to complete production tasks and the time spent completing project tasks.
  - Some form of time reporting system (either paper-based or automated time accounting mechanism)
- Measurements collected from production statistics depend greatly on the number of systems and the number of users of those systems.
  - Some organizations simply track these two values
  - Other organizations need more detailed measurements: # of users added/revoked, # of access control changes/violations, # of awareness briefings, # of incidents by category (virus or worm outbreaks), # of malicious codes blocked by filter

Collecting InfoSec Measurements

- Some thought must go into the processes used for data collection and record keeping

- Once the question of what to measure is answered
  - The how, when, where, and who questions of metrics collection must be addressed

- Designing the collection process requires consideration of the metric's intent
  - Along with a thorough knowledge of how production services are delivered

Collecting InfoSec Measurements (cont'd.)

- **Measurements Development Approach**
  - One of the priorities is determining whether the measurements used will be macro-focus or micro-focus
    - ✓Macro-focus measurements examine the performance of the overall security program
    - ✓Micro-focus measurements examine the performance of an individual controller or group of controls within the information security program
  - Or use both macro- and micro-focus measurements in a limited assessment
  - What is important is that the measurements are specifically tied to individual InfoSec goals and objectives.

Collecting InfoSec Measurements (cont'd.)

- **Measurement Prioritization and Selection**
  - As organizations seem to better manage what they measure, it is important to ensure that individual metrics are prioritized in the same manner as the processes that they measure
  - Use a simple low-, medium-, or high-priority ranking system, or a weighted scale approach, which would involve assigning values to each measurement based on its importance in the overall InfoSec program, and on the overall risk mitigation goals and the criticality of the systems
  - While there are literally hundreds of measurements that could be used, only those associated with appropriate-level priority activities should be incorporated

Collecting InfoSec Measurements (cont'd.)

- **Establishing Performance Targets**
  - Performance targets make it possible to define success in the security program
    - ✓ Many InfoSec measurements targets are represented by a 100% target goal
  - Other types of performance measurements, such as those used to determine relative effectiveness, efficiency, or impact of InfoSec on the organization's goals tend to be more subjective and will require management assessment
    - ✓ For example, the increase in relative or perceived security of the organization's information after the installation of a firewall requires a completely different perspective than that required from assessing personnel training performance through empirical measurement of attendance at training sessions or the evaluation of post-training quiz scores.

Collecting InfoSec Measurements (cont'd.)

- **Measurements Development Template**
  - NIST recommends the documentation of performance measurements in a standardized format to ensure the repeatability of the measurement development, customization, collection, and reporting activities.
  - One way to accomplish this would be to develop a custom template that an organization could use to document performance measurements that are to be used.

Candidate Measurements

- A number of example candidate measurements are provided in the table.
- Additional details on these measurements, including how they are calculated and used, are provided in NIST SP 800-55, Rev. 1.

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 operational risk assessment 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 acknowledgment 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 recognized 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 operation
Percentage of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated

Source: NIST SP 800-55, Rev. 1.

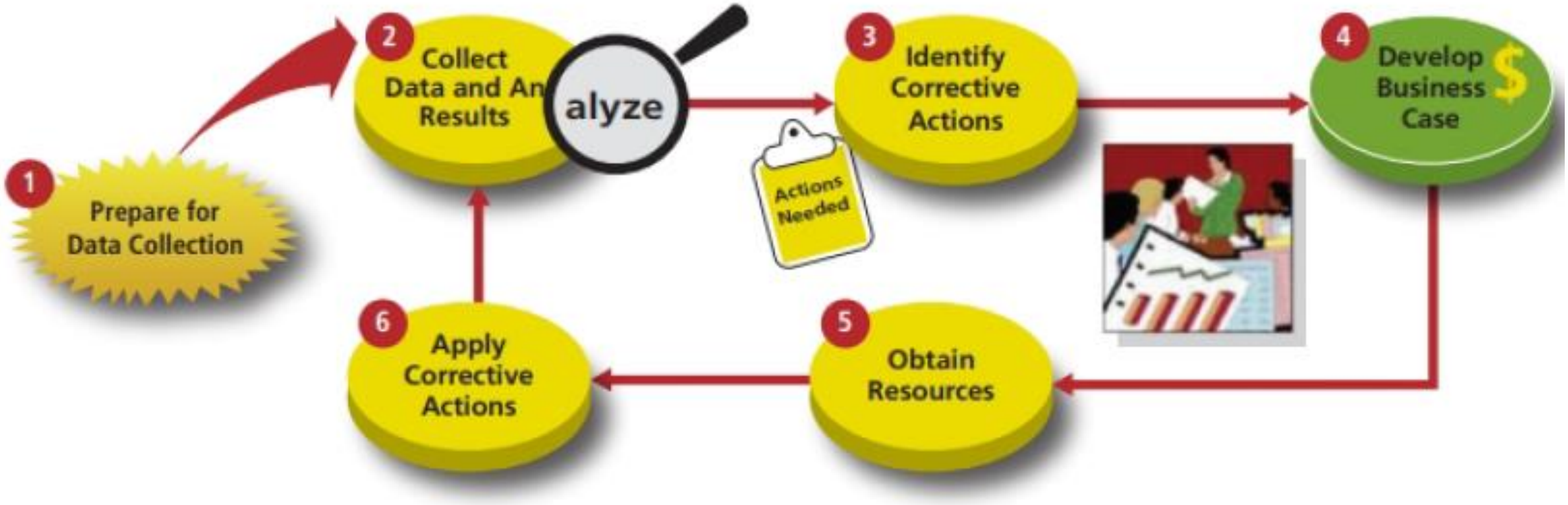
Implementing InfoSec Performance Measurement

- Once developed, InfoSec performance measurements must be implemented and integrated into ongoing InfoSec management operations.

- For the most part, it is insufficient to simply collect these measurements once (although some activities only require data collection for one particular purpose, such as those that might occur when identifying costs in a formal cost-benefit analysis, or in C&A)

- Performance measurement is an ongoing, continuous improvement operation. The collection of all measurement data should be part of standard operating procedures across the organization.

Implementing InfoSec Performance Measurement (cont'd.)



Reporting InfoSec Performance Measurements

- In most cases, simply listing the measurements collected does not adequately convey their meaning
  - For example, a line chart showing the number of malicious code attacks per day may communicate a basic fact, but unless the reporting mechanism can provide the context, e.g., the number of new malicious code variants on the Internet in that time period, the measurement will not serve its intended purpose.
- Decisions must be made about how to present correlated metrics – whether to use pie, line or bar char, and which colors denote which kinds of results.
- The CISO must also consider to whom the results of the performance measurement program should be disseminated, and how they should be delivered

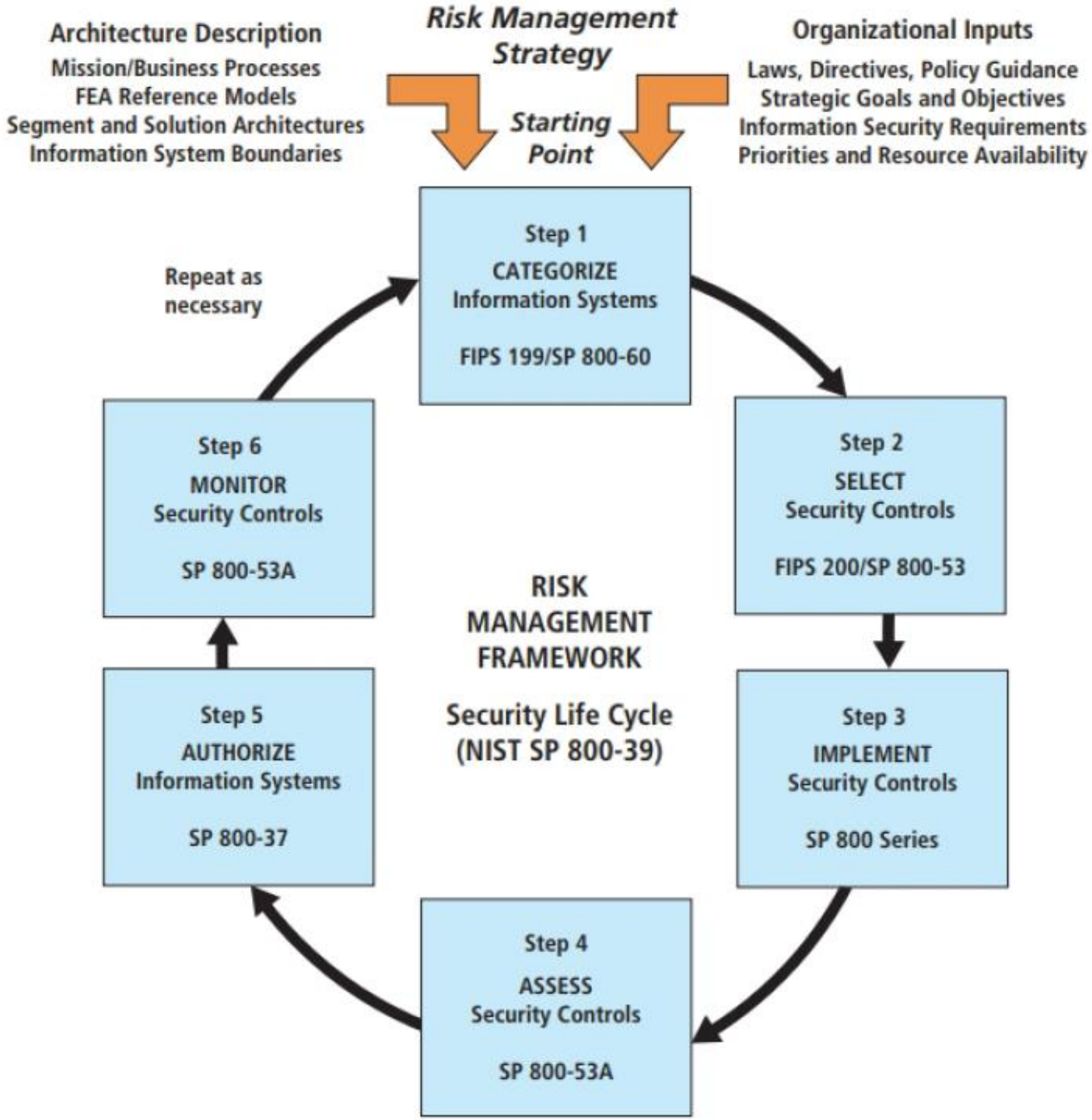
Trends in Certification and Accreditation

- **Accreditation**: 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 adequate quality
  - Challenges managers and technical staff to find the best methods to assure security

- **Certification:** a comprehensive assessment of both technical and nontechnical protection strategies for a particular system, as specified by a particular set of requirements.

Trends in Certification and Accreditation (cont'd)

- Organizations pursue accreditation or certification to gain a competitive advantage or to provide assurance or confidence to their customers.
- Prior to 2009, federal information systems required C&A
  - Accreditation, whether done by a federal agency or a private business, demonstrates that management has defined an acceptable risk level and that provided resources bring risks to that level.
- In 2009, the U.S. government, through NIST, changed the fundamental approach to the C&A of federal information systems, bringing the government into alignment with industry.
  - Focus moved from formal C&A activities to a risk-management life cycle approach.
  - With the publication of "NIST SP 800-37, Rev. 1", the approach shifted to a process of risk management-based assessment and authorization.


Architecture Description
Mission/Business Processes
FEA Reference Models
Segment and Solution Architectures
Information System Boundaries
Risk Management Strategy
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Information Security Requirements
Priorities and Resource Availability
Repeat as necessary
Step 1
CATEGORIZE
Information Systems
FIPS 199/SP 800-60
Step 2
SELECT
Security Controls
FIPS 200/SP 800-53
Step 3
IMPLEMENT
Security Controls
SP 800 Series
Step 4
ASSESS
Security Controls
SP 800-53A
Step 5
AUTHORIZE
Information Systems
SP 800-37
Step 6
MONITOR
Security Controls
SP 800-53A
RISK MANAGEMENT FRAMEWORK
Security Life Cycle
(NIST SP 800-39)

Recap

- Benchmarking is a process of following the recommended or existing practices of a similar organization or industry-developed standards. Two categories of benchmarks are used: standards of due care/due diligence and recommended practices.

- Organizations may be compelled to adopt a stipulated minimum level of security (that which any prudent organization would do), which is known as a standard of due care. Implementing controls at this minimum standard is deemed due diligence.

- Security efforts that seek to provide a superior level of performance in the protection of information are called recommended business practices or best practices. Security efforts that are among the best in the industry are termed best security practices.

Recap (cont'd)

- A practice related to benchmarking is baselining—a level of performance against which changes can be usefully compared. Baselining can provide the foundation for internal benchmarking.

- InfoSec performance management is the process of designing, implementing, and managing the use of the collected data elements called "measurements" to determine the effectiveness of the overall security program.

- There are three types of InfoSec performance measurements: 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 on the organization or its mission.

Recap (cont'd)

- 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. In recent years, the C&A approach has been replaced in federal information systems by a Risk Management Framework.