TY BTech CSE (CSF) Semester (AY 2023-2024)

Computer Science and Engineering

Disclaimer:

a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer to the references to learn about the sources, when applicable.

b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

Unit 3: Implementing Security Management

Information Security Project Management, Benchmarking, Performance Measure in Information Security Management-InfoSec Performance Measure: Management, Metrics, Building, Collecting, Implementing, Reporting, Emerging Trends in Certification and Accreditation, SP 800-37, SP 800-53, Security Management Practices and Auditing.

Information Security Project Management

Benchmarking

- 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

- Benchmarking (cont'd.)
  - Can help to 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)

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

- 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

Performance Measure in Information Security 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 Measure: Management, Metrics, Building, Collecting, Implementing, Reporting

InfoSec Performance Management

- **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

- 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

- 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

- 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

- 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?

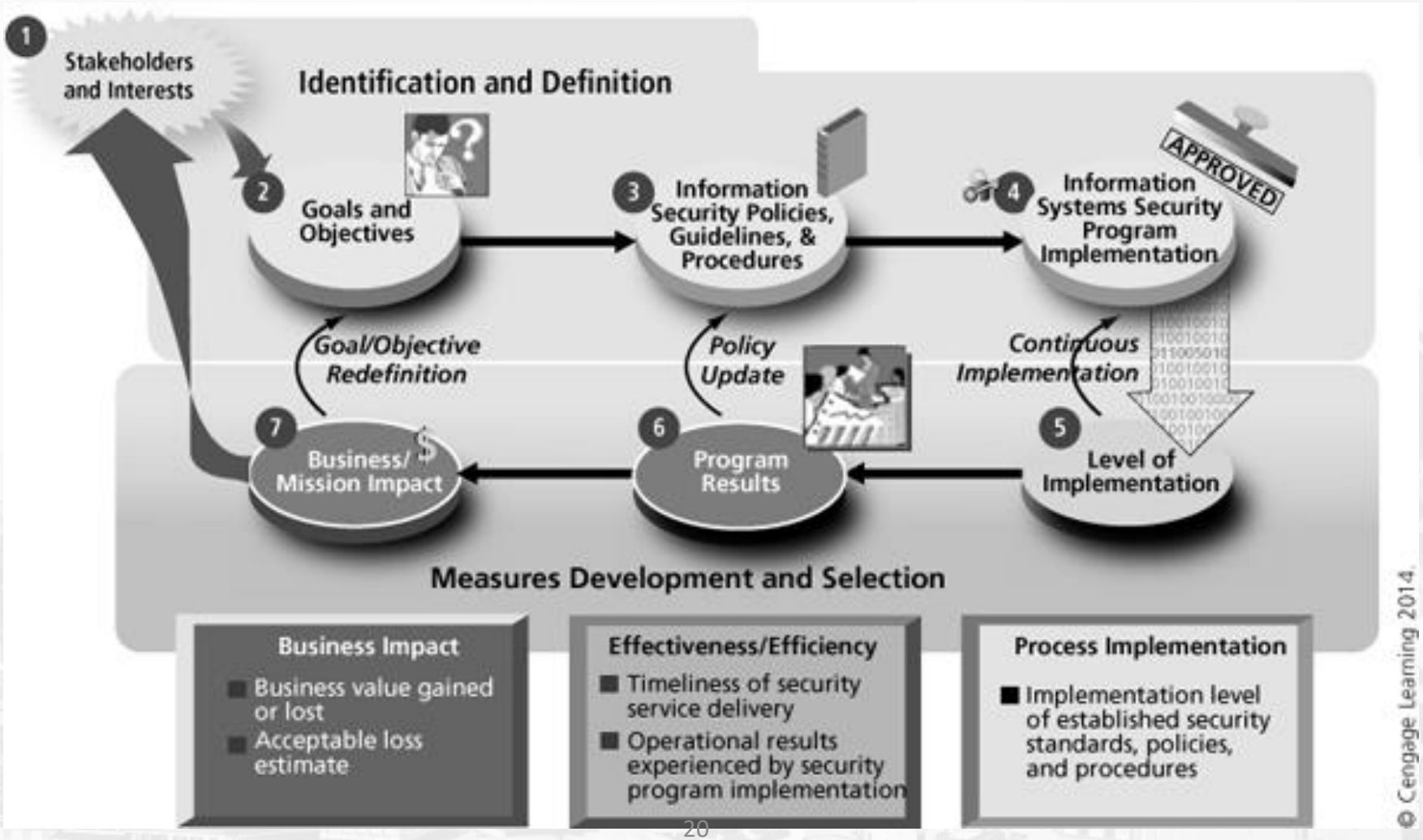
Building the Performance Measurement Program

- 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

- 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

Information security performance measurement development process



Building the Performance Measurement Program

- 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

- 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

- **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

- **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

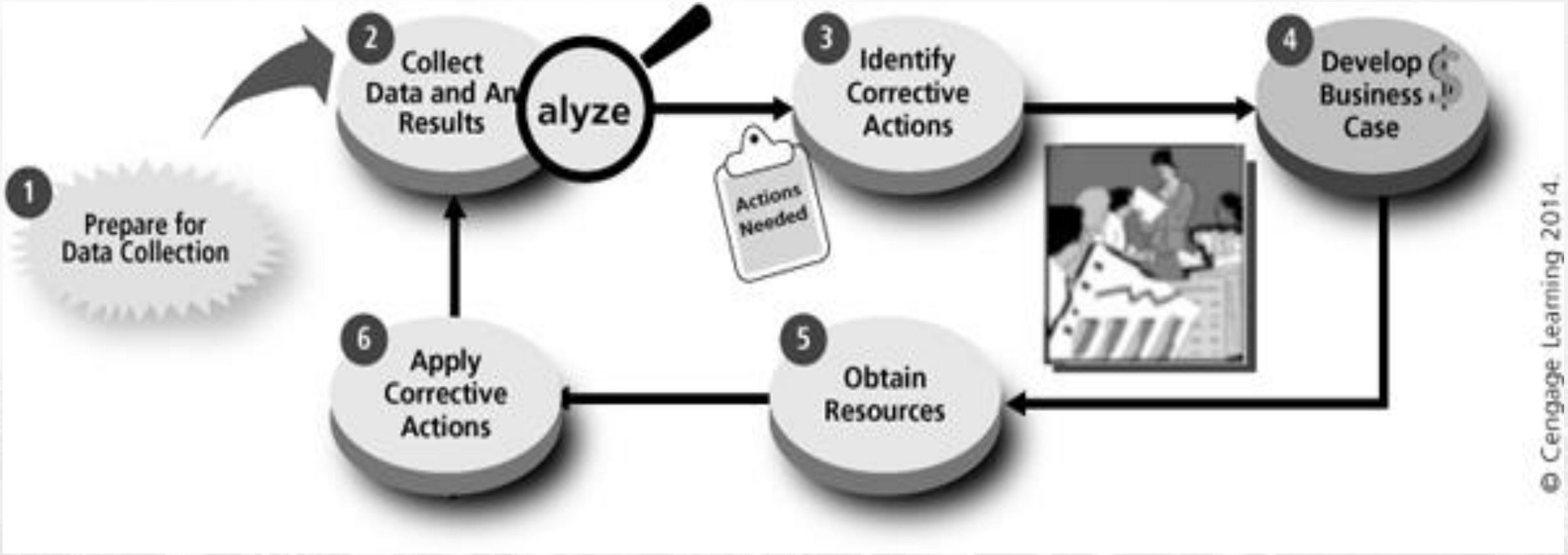
Implementing InfoSec Performance Management

- 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

- 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

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

Table 2. Measures Template and Instructions

Field	Data
Measure ID	State the unique identifier used for measure tracking and sorting. The unique identifier can be from an organization-specific naming convention or can directly reference another source.
Goal	Statement of strategic goal and/or information security goal. For system-level security control measures, the goal would guide security control implementation for that information system. For program-level measures, both strategic goals and information security goals can be included. For example, information security goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific information security goal extracted from agency documentation, or identify an information security program goal that would contribute to the accomplishment of the selected strategic goal.
Measure	Statement of measurement. Use a numeric statement that begins with the word "percentage," "number," "frequency," "average," or a similar term. If applicable, list the NIST SP 800-53 security control(s) being measured. Security controls that provide supporting data should be stated in Implementation Evidence. If the measure is applicable to a specific FIPS 199 impact level (high, moderate, or low), state this level within the measure.
Type	Statement of whether the measure is implementation, effectiveness/efficiency, or impact.
Formula	Calculation to be performed that results in a numeric expression of a measure. The information gathered through listing implementation evidence serves as an input into the formula for calculating the measure.
Target	Threshold for a satisfactory rating for the measure, such as milestone completion or a statistical measure. Target can be expressed in percentages, time, dollars, or other appropriate units of measure. Target may be tied to a required completion time frame. Select final and interim target to enable tracking of progress toward stated goal.
Implementation Evidence	Implementation evidence is used to compute the measure, validate that the activity is performed, and identify probable causes of unsatisfactory results for a specific measure. • For manual data collection, identify questions and data elements that would provide the data inputs necessary to calculate the measure's formula, qualify the measure for acceptance, and validate provided information. • For each question or query, state the security control number from NIST SP 800-53 that provides information, if applicable. • If the measure is applicable to a specific FIPS 199 impact level, questions should state the impact level. • For automated data collection, identify data elements that would be required for the formula, qualify the measure for acceptance, and validate the information provided.
Frequency	Indication of how often the data is collected and analyzed, and how often the data is reported. Select the frequency of data collection based on a rate of change in a particular security control that is being evaluated. Select the frequency of data reporting based on external reporting requirements and internal customer preferences.

Field	Data
Responsible Parties	Indicate the following key stakeholders: • Information Owner: Identify organizational component and individual who owns required pieces of information; • Information Collector: Identify the organizational component and individual responsible for collecting the data. (Note: If possible, Information Collector should be a different individual or even a representative of a different organizational unit than the Information Owner, to avoid the possibility of conflict of interest and ensure separation of duties. Smaller organizations will need to determine whether it is feasible to separate these two responsibilities.); and • Information Customer: Identify the organizational component and individual who will receive the data.
Data Source	Location of the data to be used in calculating the measure. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information.
Reporting Format	Indication of how the measure will be reported, such as a pie chart, line chart, bar graph, or other format. State the type of format or provide a sample.

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.

- Measure 1: Security Budget (program-level)
- Measure 2: Vulnerability Management (program-level)
- Measure 3: Access Control (AC) (system-level)
- Measure 4: Awareness and Training (AT) (program-level)
- Measure 5: Audit and Accountability (AU) (system-level)
- Measure 6: Certification, Accreditation, and Security Assessments (CA) (program-level)
- Measure 7: Configuration Management (CM) (program-level)
- Measure 8: Contingency Planning (CP) (program-level)
- Measure 9: Identification and Authentication (IA) (system-level)
- Measure 10: Incident Response (IR) (program-level and system-level)
- Measure 11: Maintenance (MA) (system-level)
- Measure 12: Media Protection (MP) (program-level and system-level)
- Measure 13: Physical and Environmental (PE) (program-level)
- Measure 14: Planning (PL) (program-level and system-level)
- Measure 15: Personnel Security (PS) (program-level and system-level)
- Measure 16: Risk Assessment (RA) (system-level)
- Measure 17: System and Services Acquisition (SA) (program-level and system-level)
- Measure 18: System and Communications Protection (SC) (program-level)
- Measure 19: System and Information Integrity (SI) (program-level and system-level)

Measure 2: Vulnerability Management (program-level)

Field	Data
Measure ID	Vulnerability Measure 1
Goal	• *Strategic Goal:* Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. • *Information Security Goal:* Ensure all vulnerabilities are identified and mitigated.
Measure	Percentage (%) of high[13] vulnerabilities mitigated within organizationally defined time periods after discovery NIST SP 800-53 Controls: RA-5; Vulnerability Scanning
Measure Type	Effectiveness/**Efficiency**
Formula	(Number of high vulnerabilities identified and mitigated within targeted time frame during the time period /number of high vulnerabilities identified within the time period) *100
Target	This should be a high percentage defined by the organization.
Implementation Evidence	1. Number of high vulnerabilities identified across the enterprise during the time period (RA-5)? _____ 2. Number of high vulnerabilities mitigated across the enterprise during the time period (RA-5)? _____
Frequency	Collection Frequency: Organization-defined (example: quarterly) Reporting Frequency: Organization-defined (example: quarterly)
Responsible Parties	• Information Owner: Chief Information Officer (CIO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO]), System Owner • Information Collector: System Administrator or Information System Security Officer (ISSO) • Information Customer: Chief Information Officer (CIO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])
Data Source	Vulnerability scanning software, audit logs, vulnerability management systems, patch management systems, change management records
Reporting Format	Stacked bar chart illustrating the percentage of high vulnerabilities closed within targeted time frames after discovery over several reporting periods

Measure 9: Identification and Authentication (IA) (system-level)

Field	Data
Measure ID	User Accounts Measure 1 (or a unique identifier to be filled out by the organization)
Goal	• *Strategic Goal:* Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. • *Information Security Goal:* All system users are identified and authenticated in accordance with information security policy.
Measure	Percentage (%) of users with access to shared accounts NIST SP 800-53 Controls – AC-2: Account Management, AC-3: Access Enforcement, and IA-2: User Identification and Authentication
Measure Type	**Effectiveness**/Efficiency
Formula	(Number of users with access to shared accounts/total number of users) *100
Target	This should be a low percentage defined by the organization.
Implementation Evidence	1. How many users have access to the system (IA-2)? _____ 2. How many users have access to shared accounts (AC-2)? _____
Frequency	Collection Frequency: Organization-defined (example: monthly) Reporting Frequency: Organization-defined (example: monthly)
Responsible Parties	• Information Owner: Organization-defined (example: System Owner, System Administrator) • Information Collector: Organization-defined (example: System Administrator) • Information Customer: Chief Information Officer (CIO), Information System Security Officer (ISSO), Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])
Data Source	Configuration Management Database, Access Control List, System-Produced User ID Lists
Reporting Format	Pie chart comparing the percentage of users with access to shared accounts versus the percentage of users without access to shared accounts

5 Core Documents of NIST

- NIST SP 800-30, Guide for Conducting Risk Assessments.
- NIST SP 800-37, Risk Management Framework for Information Systems and Organizations.
- NIST SP 800-39, Managing Information Security Risk.
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems.
- NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations.

NIST SP 800-53 Rev. 1

- The National Institute of Standards and Technology (NIST) information technology laboratory is responsible for developing the NIST CSF, the gold standard cybersecurity framework. NIST Special Publication 800-53 operates as one of the forefront cybersecurity guidelines for federal agencies in the United States to maintain their information security systems. These guidelines protect the system's security and the sensitive data of the citizens being served.
- NIST SP 800-53 has had five revisions and comprises over 1000 controls. This catalog of security controls allows federal government agencies the recommended security and privacy controls for federal information systems and organizations to protect against potential security issues and cyber attacks.

- NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems.
- Guidance on how to use a FIPS Publication 199 security categorization to identify minimum security controls for an information system.
- Minimum (baseline) security controls for low, moderate, and high impact information systems.
- A catalog of security controls for information systems requiring additional threat coverage.

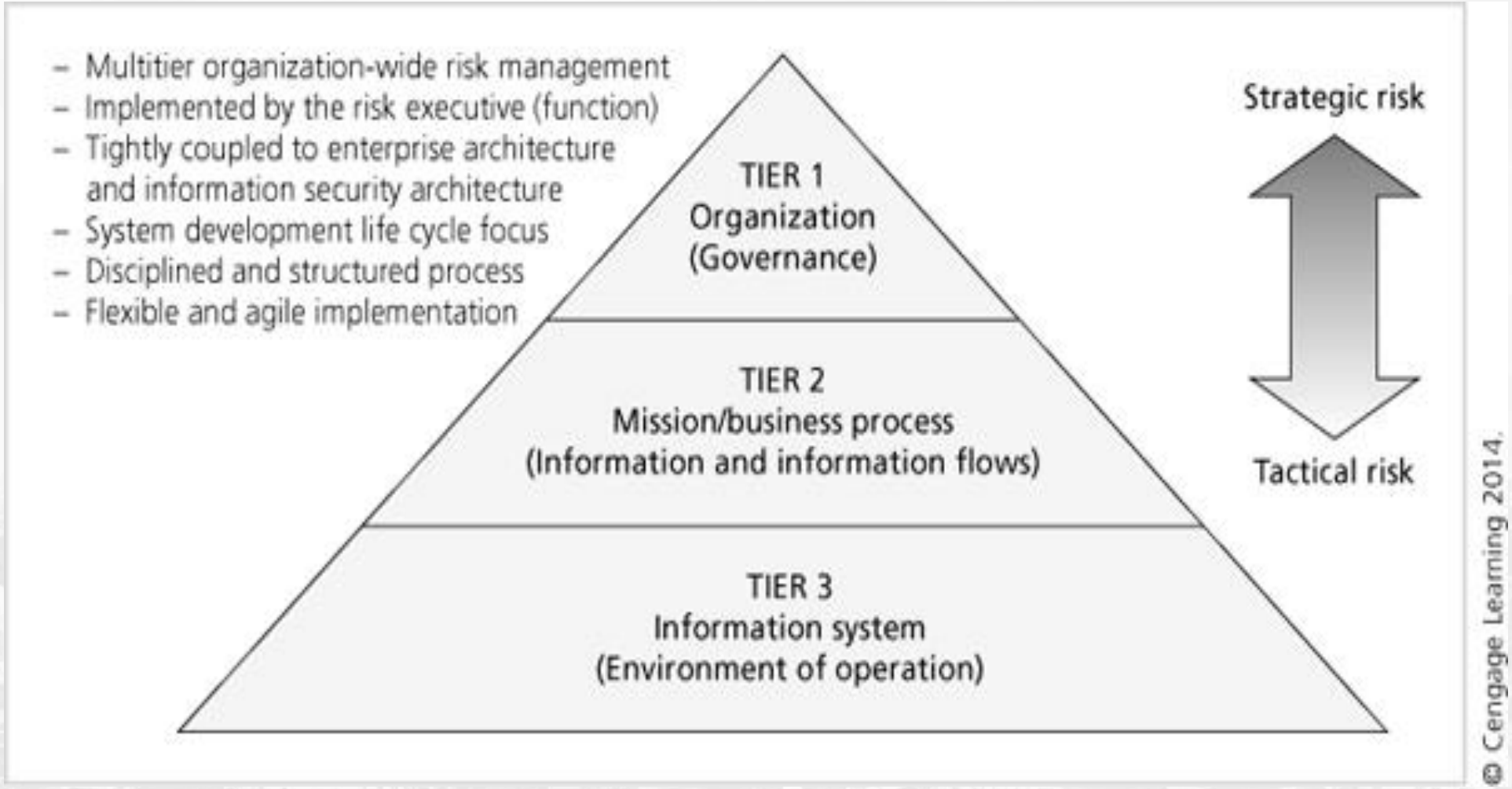
Security Control families

- AC - Access Control
- AU - Audit and Accountability
- AT - Awareness and Training
- CM - Configuration Management
- CP - Contingency Planning
- IA - Identification and Authentication
- IR - Incident Response
- MA - Maintenance
- MP - Media Protection
- PS - Personnel Security
- PE - Physical and Environmental Protection
- PL - Planning
- PM - Program Management
- RA - Risk Assessment
- CA - Security Assessment and Authorization
- SC - System and Communications Protection
- SI - System and Information Integrity
- SA - System and Services Acquisition

NIST SP 800-37 Rev. 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

Tiered risk management approach



NIST SP 800-37 Rev. 1

- 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

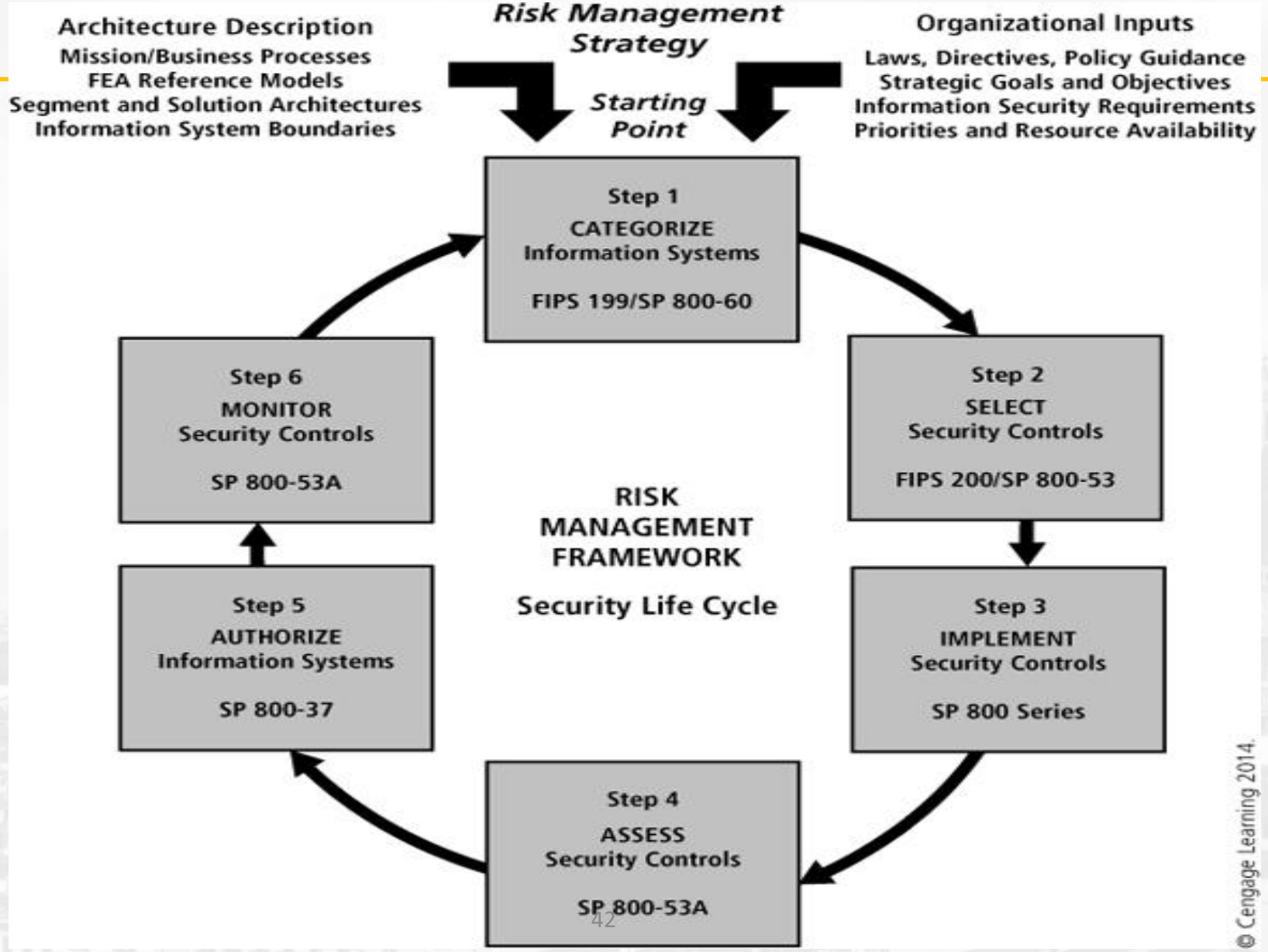
  3) **Implement** the security controls and describe how the controls are employed within the information system.

  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

Risk management framework



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.
  - Formal declaration by the Designated Approving Authority(DAA) that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
- **Certification** - a comprehensive assessment of both technical and nontechnical protection strategies for a particular system.
  - Certification: Comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements.

- Organizations pursue accreditation or certification to gain a competitive advantage or to provide assurance or confidence to their customers.
- Accreditation and certification are not permanent.
  - Most accreditation and certification processes require reaccreditation or recertification every few years

Certification vs Accreditation

Comparison Table

Characteristics	Certification	Accreditation
Definition	Refers to a written assurance by a third party on the conformity of a service, product or process, based on certain specified requirements provided by some form of education, audit, assessment or external review	Refers to formal recognition on the competency towards specified standards by an authoritative body.
Base activities	Relates to all company activities in a given industry	Is based on specific activities, and is not based on all activities in an organization
Endorsements	Involves the endorsement of a product, service or proccess by a third party	Involves the endorsement of a product, service or process by an independent third party.

Security Management Practices and Auditing

- A security audit, also known as a cybersecurity audit, is a comprehensive assessment of your organization's information systems; typically, this assessment measures your information system's security against an audit checklist of industry best practices and/or federal regulations.
- A comprehensive security audit will assess an organization's security controls relating to the following:
  - Physical components of your information system and the environment in which the information system is housed.
  - Applications and software, including security patches your systems administrators, have already implemented.
  - Network vulnerabilities, including public and private access and firewall configurations.
  - The human dimension, including how employees collect, share, and store highly sensitive information.
  - The organization's overall security strategy, including security policies, organization charts, and risk assessments.

- A security audit works by testing whether your organization's information systems are adhering to a set of internal or external criteria regulating data security, network security, and infrastructure security.
- Internal criteria include your company's IT policies, procedures, and security controls.
- External criteria include federal regulations like the Health Insurance Portability and Accountability Act (HIPAA) and COSO, and standards set by the International Organization for Standardization (ISO) or the National Institute for Standards in Technology (NIST).
- A security audit consists of a complete assessment of all components of your IT infrastructure — this includes operating systems, servers, digital communication and sharing tools, applications, data storage and collection processes, third-party providers, and more.

- Companies need regular security audits to make sure they are properly protecting their clients' personel information, complying with federal regulations, and avoiding liability and costly fines. To avoid penalties, companies need to keep up with ever-changing federal regulations
- Periodic security audits are necessary to make sure your organization is up to speed with any new requirements.
- A full security audit often involves auditors both internal or external to the organization, and the steps depend on the external security compliance measures your organization must meet.

- In general, a security audit will involve **interviews with stakeholders** to understand the sensitive data contained within IT systems (and even physical locations, like data centers), the security controls in place to protect that data, and how the IT infrastructure works together.
- These interviews might also cover the wider IT environment, including perimeter firewalls, any previous data breaches, and any recent incidents. These interviews are often called “walkthroughs.” Some auditors may also want to observe controls being executed in real-time.
- In a security audit, expect the audit team to request certain documents and logs to review, including relevant security policies, checklists, diagrams, and tickets. They will inspect these artifacts to determine if security practices are being carried out according to policy.
- There are a number of computer-assisted audit techniques (CAATs) on the market designed to automate your audit process. CAATs regularly run through the steps of an audit, seeking out vulnerabilities and automatically preparing audit reports. However, always have a trained IT manager or professional auditor reviewing these reports.

Summary

- 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

- 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

- 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

- Management of Information Security, 4th Edition

Tutorial 1