Lecture 7: Security Management Practices

EECS 711 Security Management & Audit

Objectives

- Elements of key information security management practices
- Key components of a security metrics program
- Suitable strategies for the implementation of a security metrics program
- Emerging trends in the certification and accreditation

TOPIC 7.1 BENCHMARKING

Benchmarking

- **Benchmarking**
  - a business term
  - “the process of comparing one’s business processes and performance metrics to industry bests and best practices from other companies” [Wikipedia]
- **InfoSec Benchmarking**
  - to create a security blueprint from paths taken by similar organizations
  - help determine which controls should be considered, but cannot determine how controls should be implemented

Benchmarking

- Two categories of benchmarks
  - **Recommended practices**
    - a.k.a. best security practices
    - “gold standard” – the best of the best
  - **Standards of due care and due diligence**
    - a.k.a. due care and due diligence
    - legal/financial/personnel constraints
    - reasonable level of security in all areas
      - “good security now is better than perfect security never”

Benchmarking

- **Standard of Due Care**
  - "provide a framework that helps to define a minimum standard of protection that business stakeholders must attempt to achieve" [CISSP Study Guide]
    - Prudent Man Rule – assess planned actions by considering what would be reasonable if done by another similar and prudent organization in similar circumstances
  - set a required minimal level of security for a legal defense
    - lack of due care is often considered "negligence"

Benchmarking

- **Standard of Due Diligence**
  - the management of due care
  - implement and maintain controls at the minimum standard
  - requires an organization to ensure the implemented standards continue to provide the required level of protection
- Failure to support a standard of due care and due diligence can expose an organization to legal liability
  - showing exercising due diligence in investigating potential risks and threats and acting prudently in protection

Benchmarking

- **Example:** Web server management
  - Due care?
    - IT security policy
    - Change control policy: patch update, hotfix
    - Detection: monitoring websites
    - Correction: identify compromise and take actions (user, password)
    - …
  - Due diligence?
    - Investigate threats for IIS service (web, forums, mailing lists, …)
    - Investigate affected application (SSL, PHP/ASP, DB, …)
    - Investigate protection mechanisms
    - Performance analysis
    - Design policies
    - …

Benchmarking

- **Recommended Practices**
  - *a.k.a.* **Best Security Practices (BSP)**
  - security efforts that seek to provide a superior level of performance in the protection of information
  - security efforts that are among the best in the industry
  - balanced
    - need for information access vs. need for adequate protection
    - needs vs. being fiscally responsible
    - protecting areas: not the best in all areas; need to meet minimum standards in protecting all information assets

Benchmarking

- **Federal Agency Security Project (FASP)**
  - initiated by the federal Chief Information Officer (CIO) Council's *Federal Best Security Practice (BSP)* pilot effort
  - to identify, evaluate, and disseminate best practices for critical infrastructure protection
  - NIST developed the FASP website (2001-2015)
    - examples of agency policies, procedures, and practices
    - CIO Council's pilot BSPs, and a FAQ section
    - agencies are encouraged to submit their InfoSec practices to share with others
    - can be applied in both the public and private sectors
    - outdated and no longer maintained: FASP Archive

Benchmarking

- FASP Areas (Table 7-1 on page 250 shows Federal BSPs)
  - Audit Trails
  - Authorize Processing (C&A)
  - Contingency Planning
  - Continuous Monitoring
  - Data Integrity
  - Hardware and System Software Maintenance
  - Identification and Authentication
  - Incident Response Capability
  - Life Cycle
  - Logical Access Controls

Benchmarking

- FASP Areas (continued)
  - Network Security
  - Personnel Security
  - Physical and Environmental Protection
  - Policy and Procedures
  - Production, Input/Output Controls
  - Program Management
  - Review of Security Controls
  - Risk Management
  - Security Awareness, Training and Education
  - System Security Plan

Best Practices Example

- **PCI DSS**: Payment Card Industry Data Security Standards
  - created by PCI SSC (Security Standards Council)
  - for organizations that store, process, and transmit cardholder data
  - to increase controls over cardholder data to reduce fraud
  - compliance validation can be done by doing external Report on Compliance or Self-Assessment Questionnaire
  - PCI SSC provides best practices guidelines
    - Best Practices for Maintaining PCI DSS Compliance
    - Best Practices for Implementing a Security Awareness Program
    - More best practices are available

Selecting Recommended Practices

- Implementing best practices is not easy
  - different industries must provide different levels of compliances
  - some industries
    - regulated by laws: government agencies
    - under industry requirements: healthcare, banking, finance, petrochemical, etc.
    - government and industry **guidelines** are *required*
  - for other organizations, use as excellent info sources to control risks

Selecting Recommended Practices

- **Sources** of information on recommended practices
  - **NIST** Practices: Computer Security Resource Center
    - csrc.nist.gov
    - SP 800-53 Rev. 4; SP 800-53A Rev. 1
    - NIST SP 800-27 Rev. A: a Baseline for Achieving Security
  - **CERT/CC** Website: CMU Computer Emergency Response Team Coordination Center
    - www.cert.org
  - Industry vendors
    - Microsoft, Oracle, Cisco, etc.
  - Professional societies
    - www.techforum.com, www.securityforum.org, iapsc.org,

Selecting Recommended Practices

- Consider questions:
  - 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 as the target?
    - is your organizational structure similar to the target?
    - are you in a similar threat environment as the target?
  - can your organization expend resources at the level required by the recommended practice?

Limitations

- Benchmarking and Best Practices **limitations:**
  1. No motivation to share
     - organizations don't talk to each other
     - keep failure secret, avoid negative consequences
     - valuable lessons are not recorded, disseminated, and evaluated

  need change!
     - **professional associations and societies**: security administrators can share lessons learned
     - **public dissemination**: security journals, remove identifying details

Limitations

- Benchmarking and Best Practices **limitations:**
  2. Organizations differ
     - in size, composition, management philosophy, organizational culture, technology infrastructure planned expenditures, …
     - security is a managerial and personnel problem than a technical problem
  3. Recommended practices are a moving target
     - must keep abreast of new threats, methods, techniques, policies, guidelines, technologies, educational and training approaches

Baselining

- **Baseline**
  - an assessment of the performance of some action/process
  - a performance measure: used to usefully compare the current performance against a prior or an intended value
- **Baselining**
  - the process of measuring against an established standard
  - current security activities/events vs. prior performance
    - gather information from the first risk assessment to set up the baseline for future comparisons
  - combine baselining and benchmarking approaches for effective design

TOPIC 7.2 PERFORMANCE MEASUREMENT

InfoSec Performance Management

- *Are benefits and performance of InfoSec measurable?*
  - need effective performance metrics
  - **Performance Measurements**
    - *data points* or *trends* indicating the effectiveness of security countermeasures or controls
  - **InfoSec Performance Management**
    - the process of designing, implementing, and managing the use of the collected data points
    - to determine the effectiveness of overall program
    - to document due diligence: organizations need to show they are taking effective steps to control risk

InfoSec Performance Management

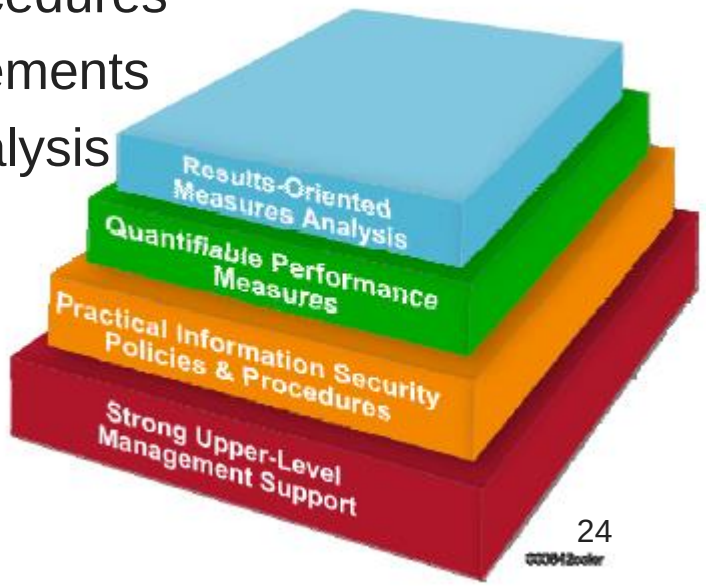
- **Performance measurements** are used to assess technical and managerial controls
  - support managerial decisions
  - increase accountability of InfoSec performance
  - improve effectiveness of InfoSec activities
  - demonstrate compliance with laws, rules, regulations
  - provide quantifiable inputs for resource allocation decisions

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

InfoSec Performance Management

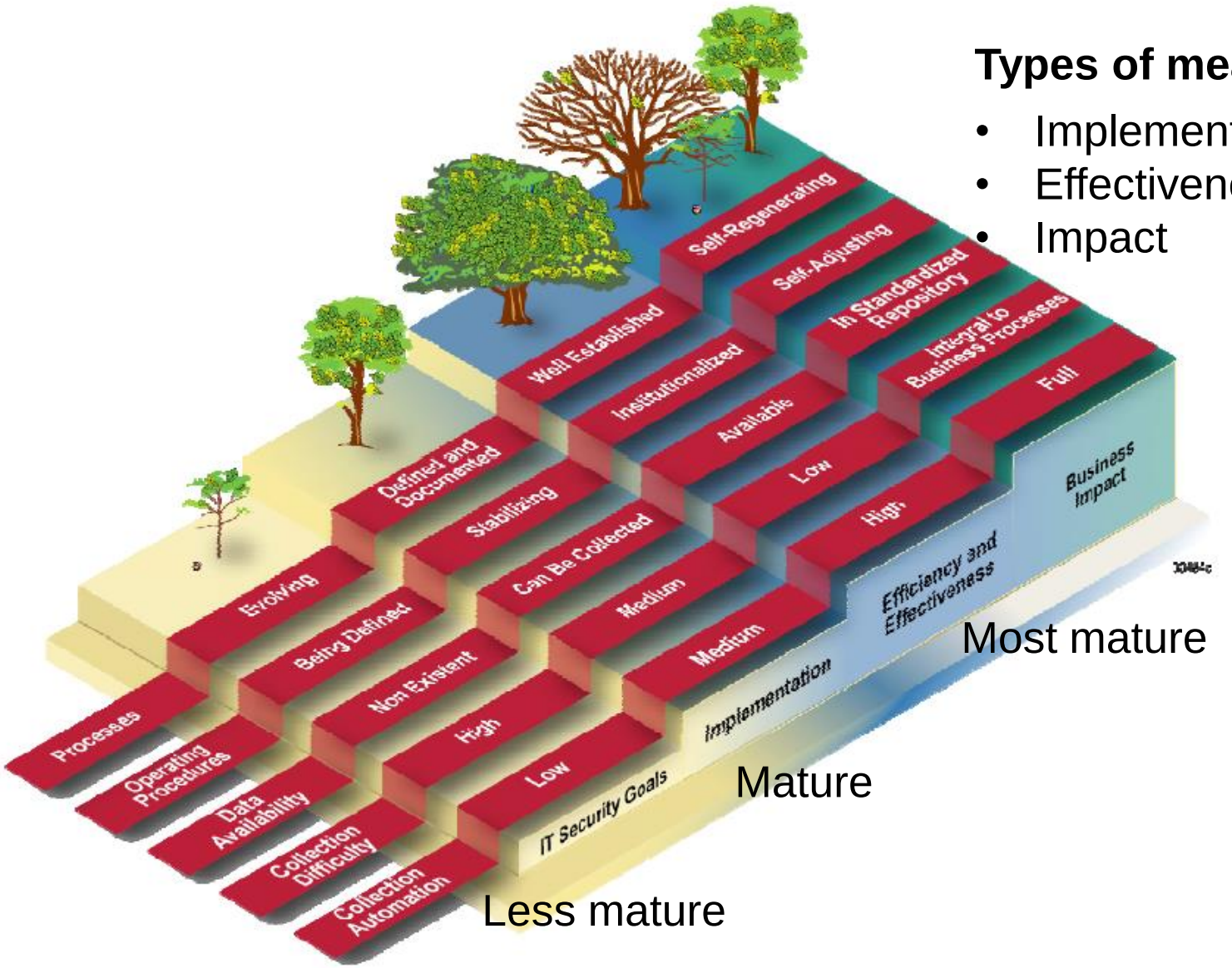
- NIST suggests the **factors** and **components** to be considered in developing the performance management program
  - For program management
    - strong upper-level management support
    - practical InfoSec policies and procedures
    - quantifiable performance measurements
    - results-oriented measurement analysis



InfoSec Performance Management

- NIST suggests the **factors** and **components** to be considered in developing the performance management program
  - For measurements
    - 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

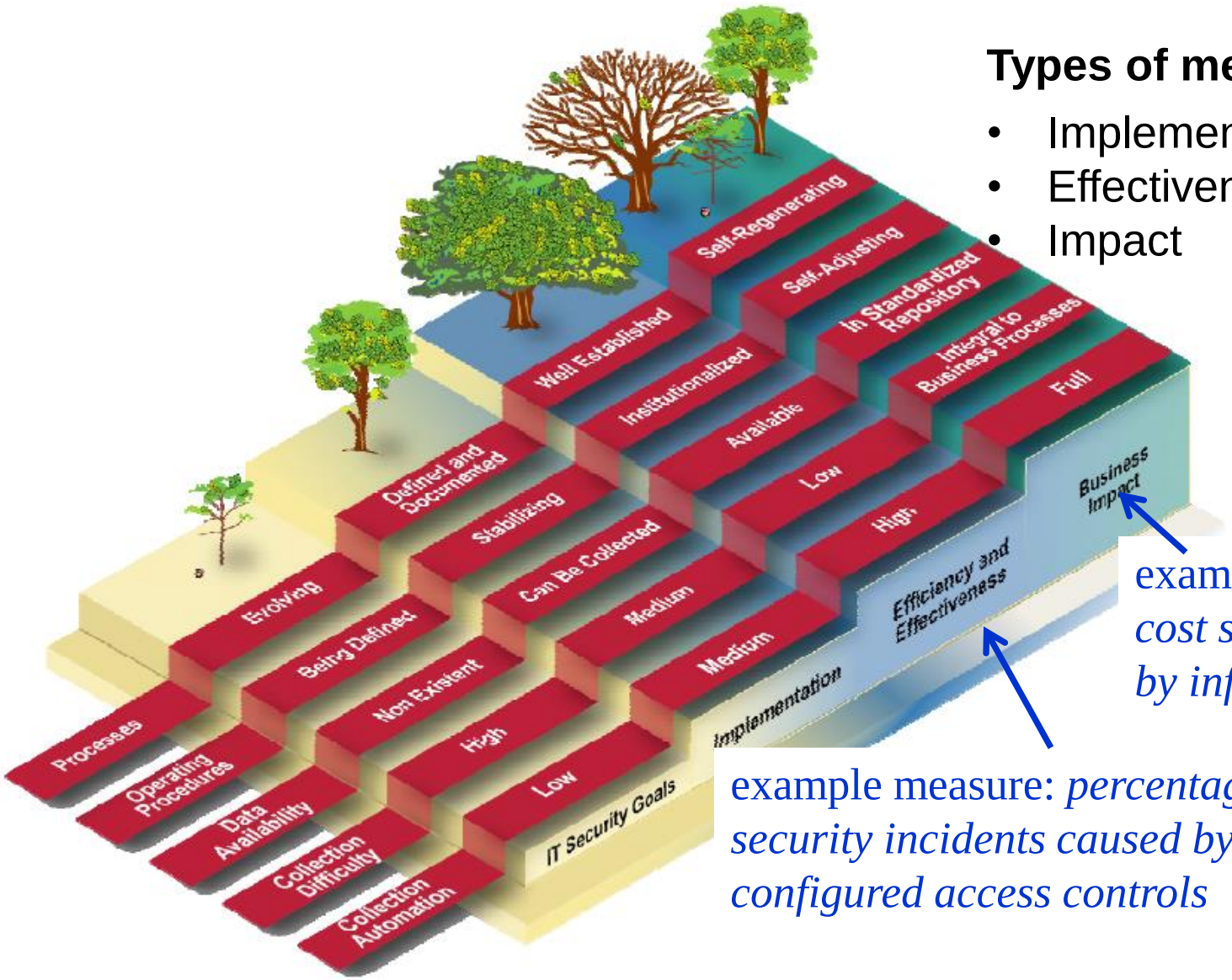
InfoSec Performance Management



Types of measures

- Implementation
- Effectiveness/efficiency
- Impact

InfoSec Performance Management



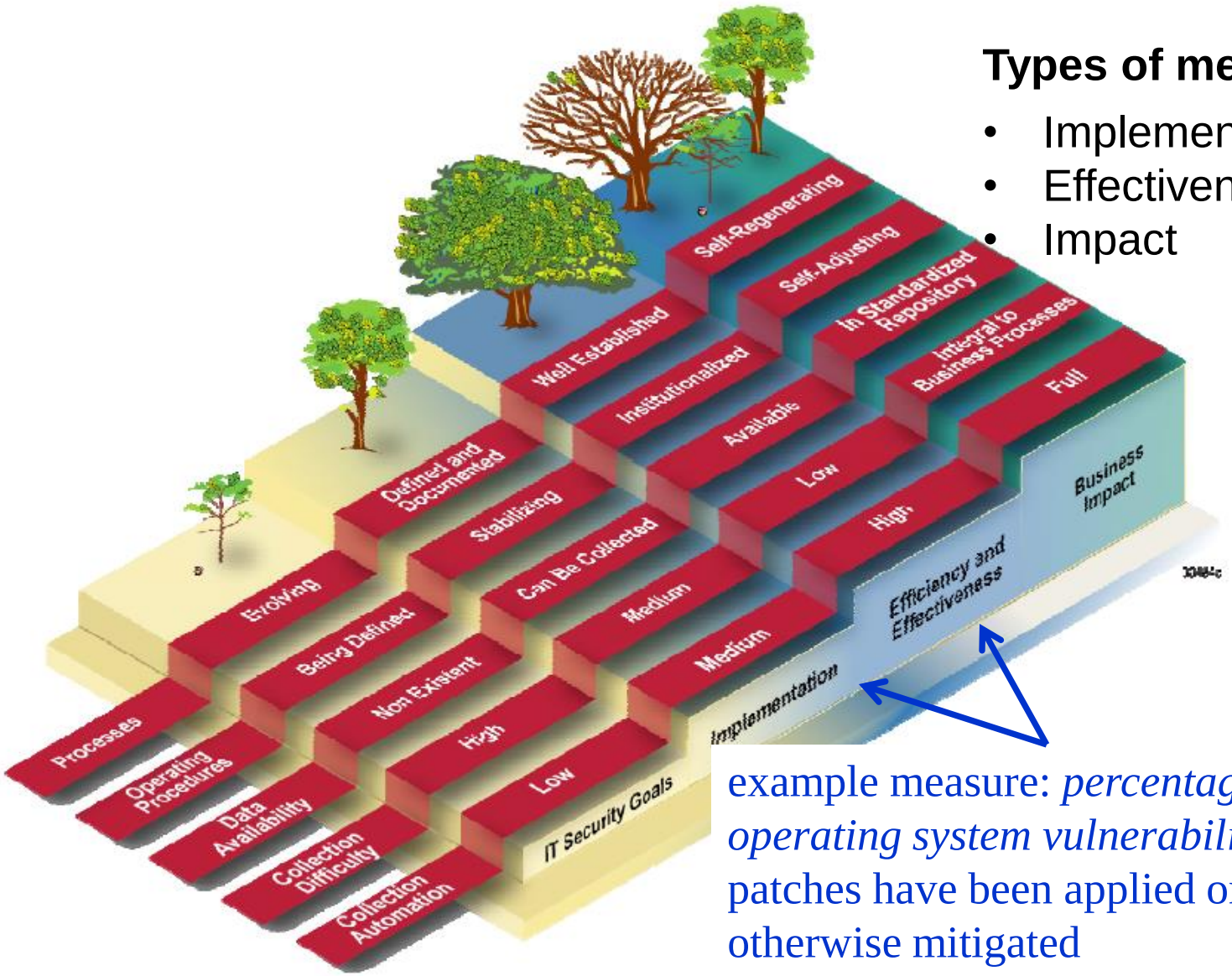
Types of measures

- Implementation
- Effectiveness/efficiency
- Impact

example measure: *cost savings produced by infosec progam*

example measure: *percentage of information security incidents caused by improperly configured access controls*

InfoSec Performance Management



Types of measures

- Implementation
- Effectiveness/efficiency
- Impact

example measure: *percentage of enterprise operating system vulnerabilities* for which patches have been applied or that have been otherwise mitigated

InfoSec Metrics

- InfoSec **Metrics**
  - enable organizations to measure the level of effort required to meet the stated objectives
    - effort consumes resources: time, hardware cycles, special software, …
    - effort needs to be periodically and constantly reviewed

what specific measurements will be collected?

why should these measurements be collected?

how will these measurements be collected?

when will these measurements be collected?

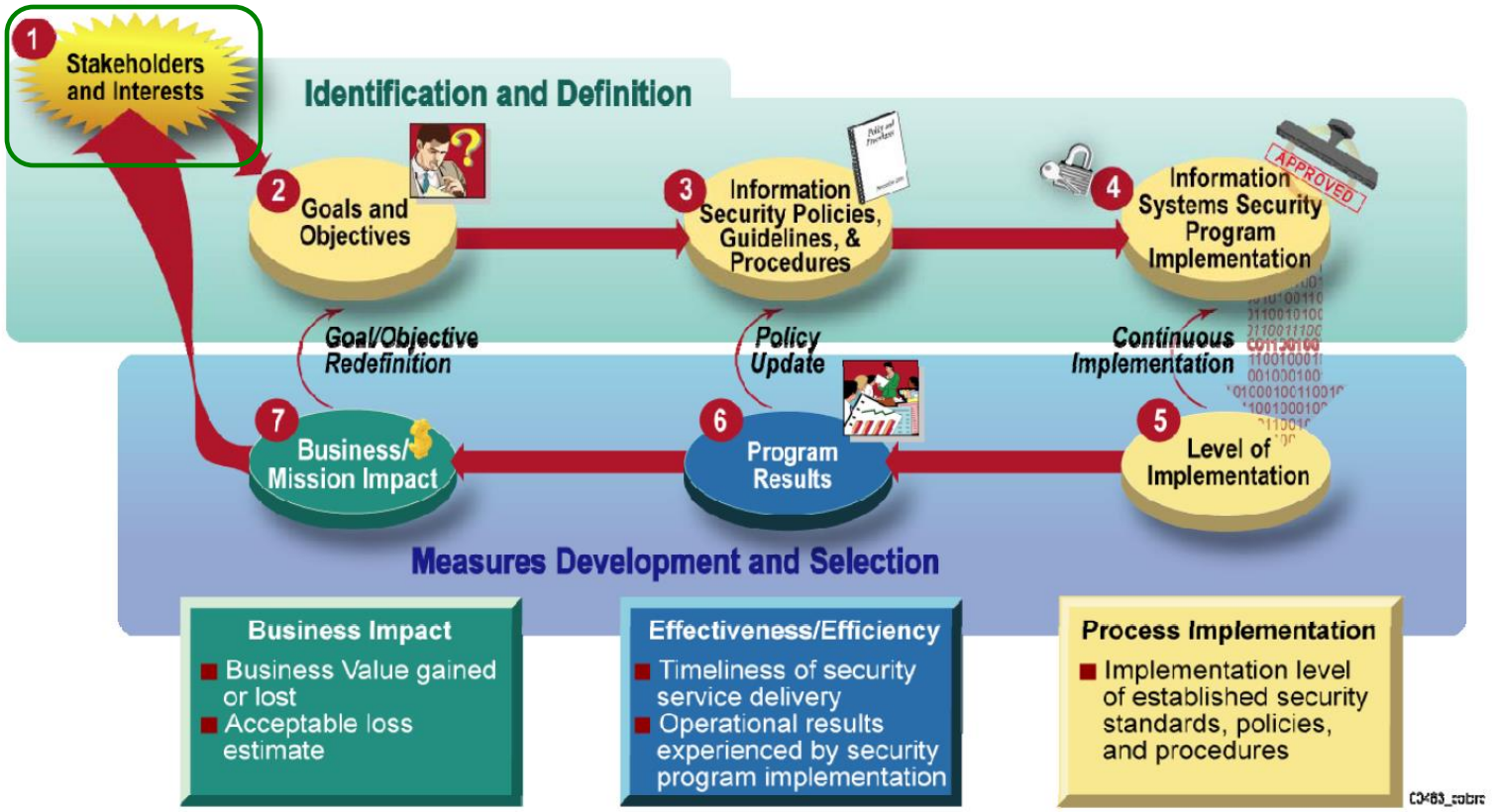
who will collect these measurements?

where (at what point in the function's process) will these measurements be collected?

How to Build?

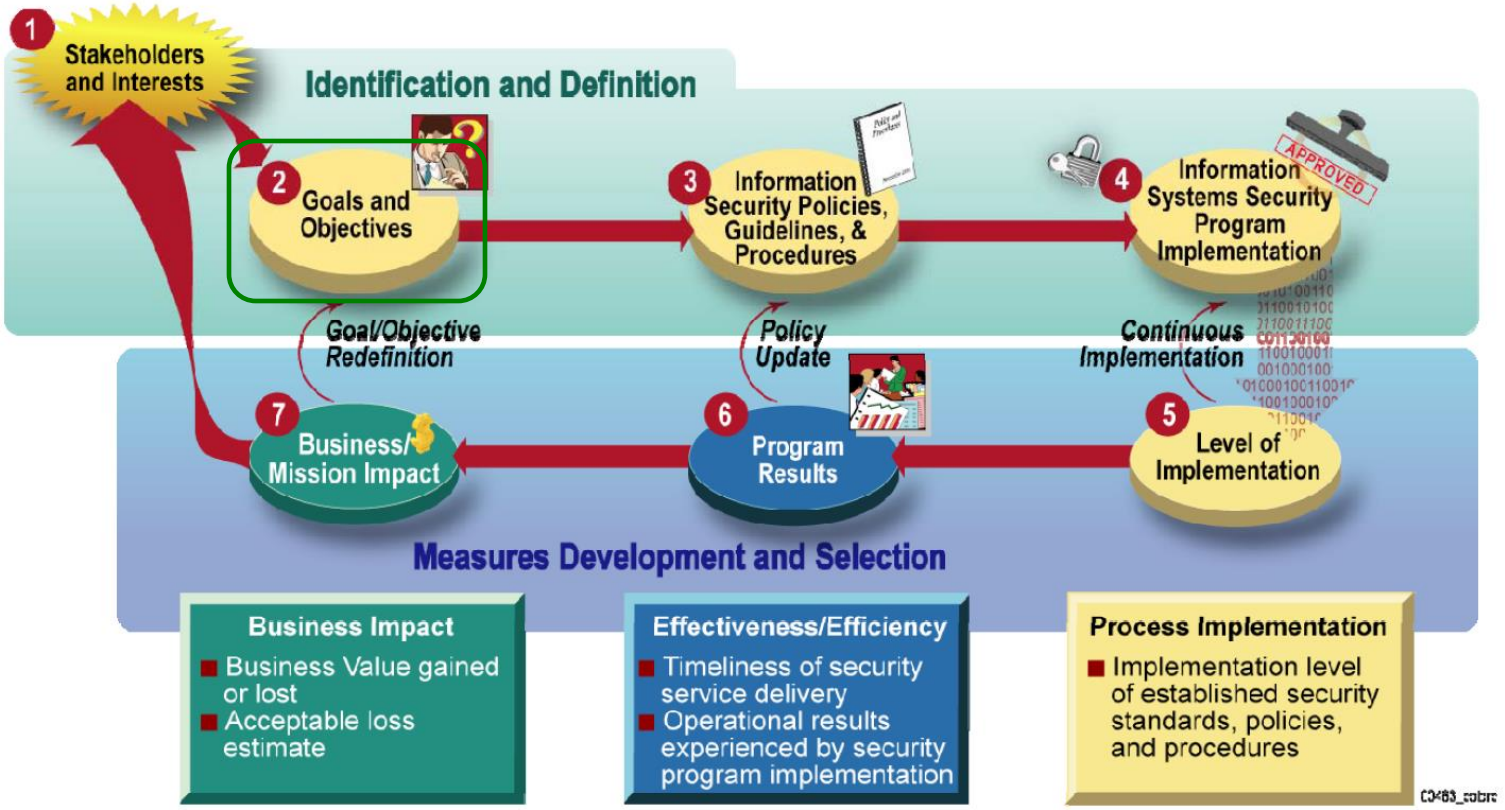
- A popular performance measurement approach
  - **NIST's SP 800-55, Rev. 1***: Performance Measurement Guide for InfoSec*
  - Two major **activities**
    - Identification and definition of the current InfoSec program
    - Development and selection of specific measurements to gauge the implementation, effectiveness, efficiency, and impact of the security controls
  - Further divided into **seven phases**
    - **not** necessarily sequentially

PM Development Process



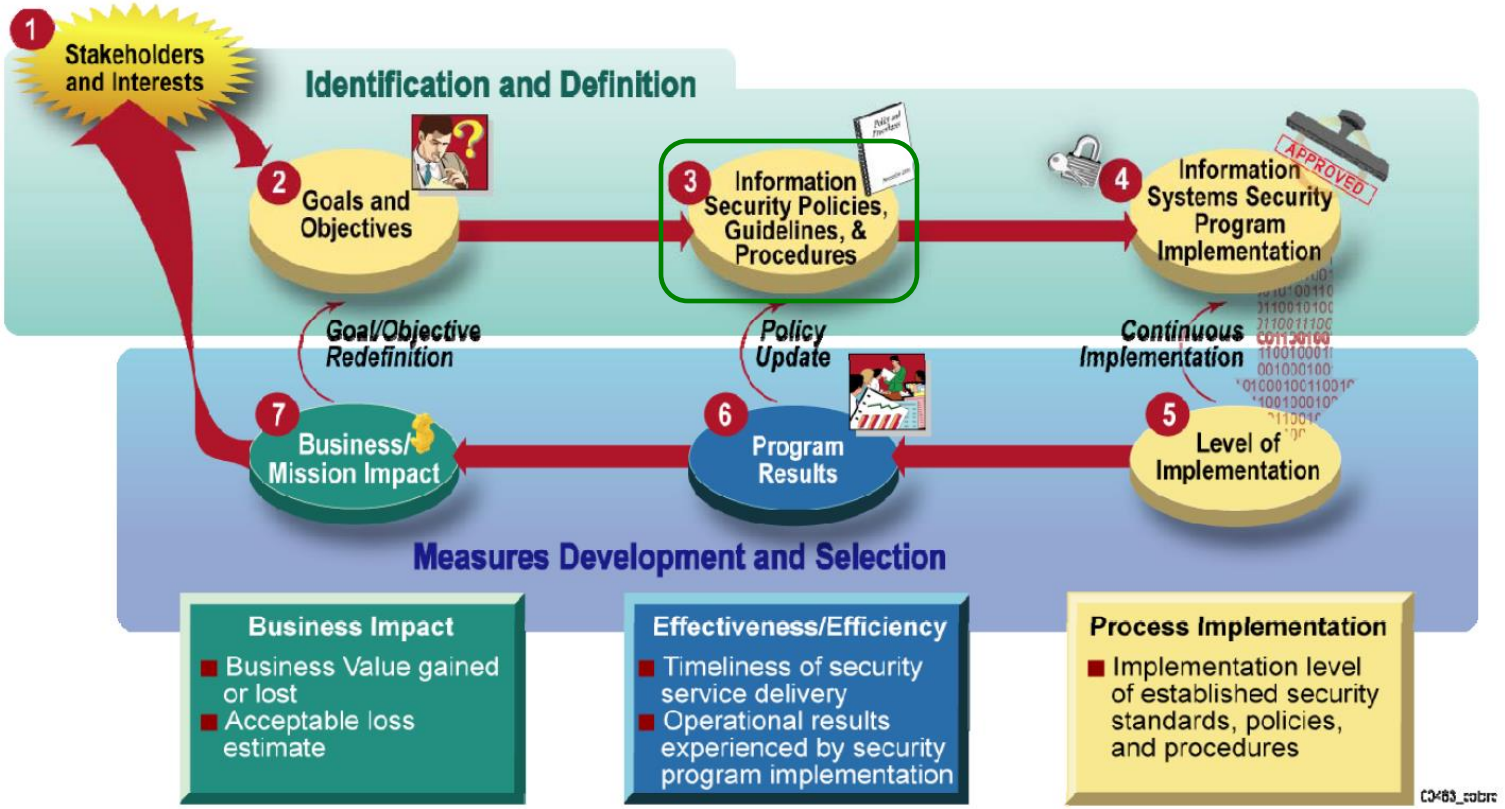
- **Phase 1:** identify relevant stakeholders and their interests in InfoSec measurement

PM Development Process



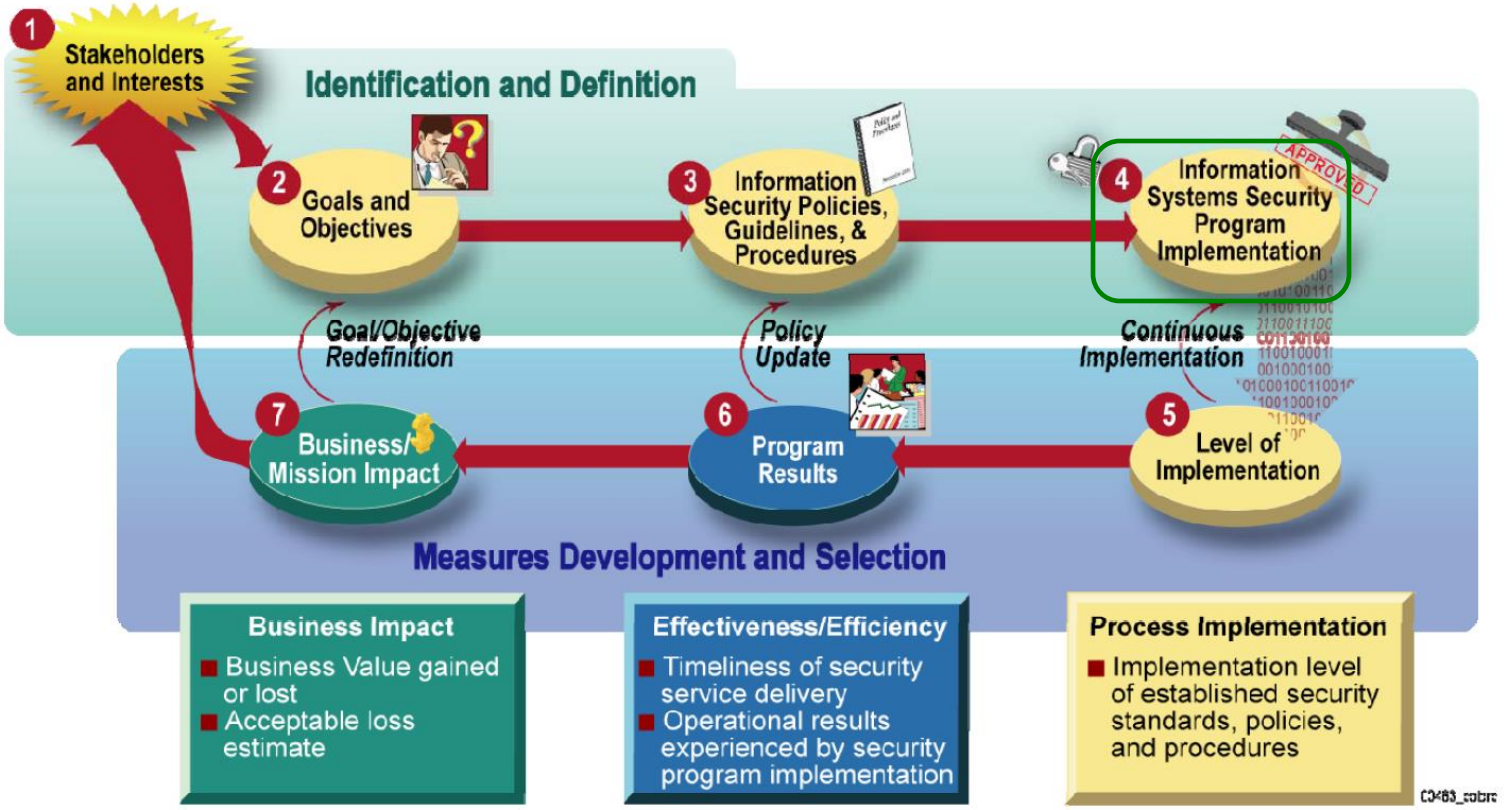
- **Phase 2:** identify and document the InfoSec performance goals and objectives that would guide security control implementation for InfoSec (FIPS 200, NIST 800-53)

InfoSec Performance Measurement Development Process



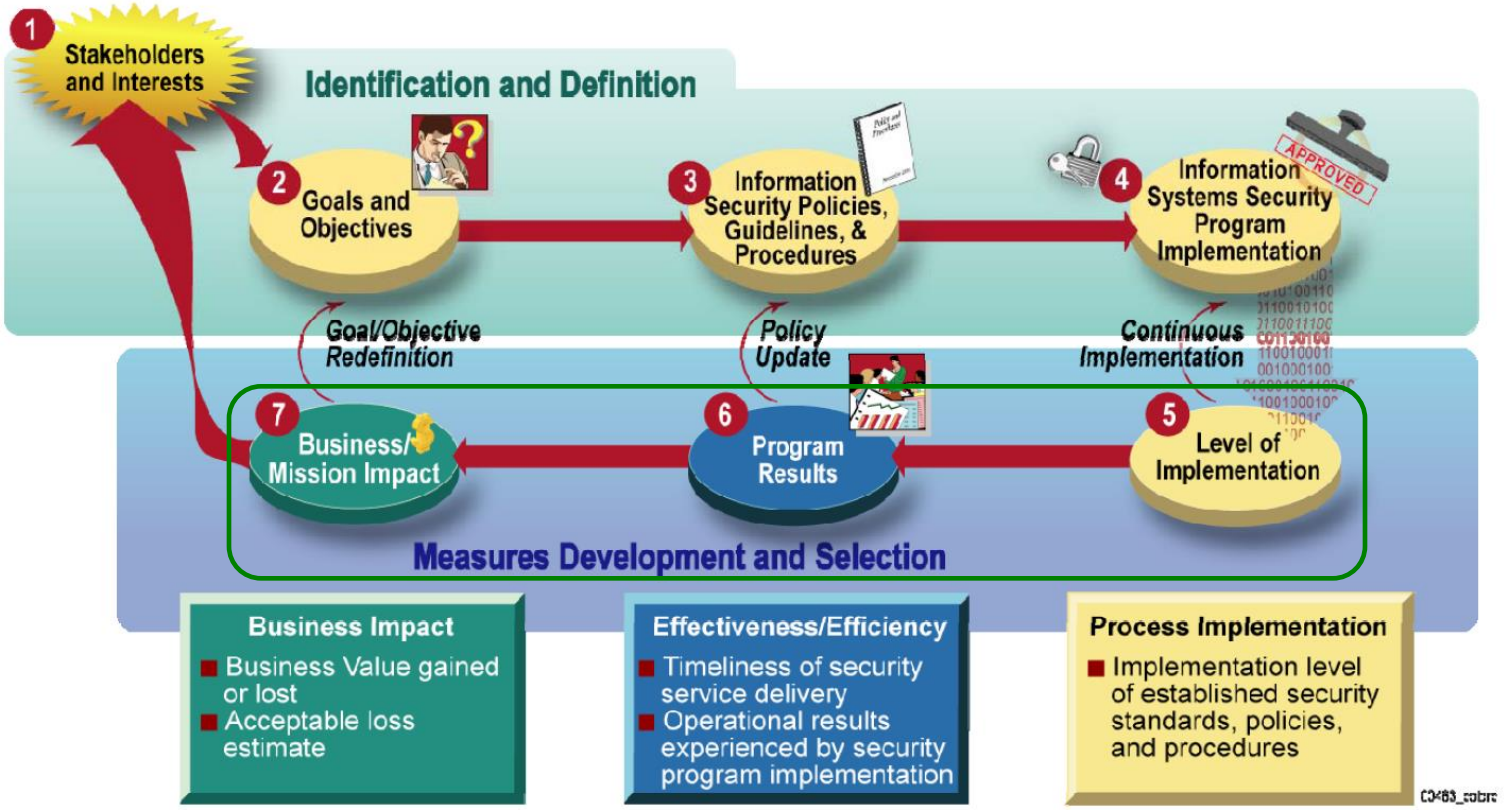
- **Phase 3:** focus on organization-specific InfoSec practices
  - Details of security control implementation
  - Baseline of InfoSec practices

InfoSec Performance Measurement Development Process



- **Phase 4:** review of existing measurements and data repositories
  - Identify appropriate implementation evidence

InfoSec Performance Measurement Development Process



- **Phases 5, 6, and 7:** develop measurements that track process implementation, efficiency/effectiveness, and mission impact

Example Candidate Measurements

- **Implementation**
  - (**Awareness & Training**): Percentage of information systems personnel that have received security training
  - (**Configuration Management**): Percentage of approved and implemented configuration changes identified in the latest automated baseline configuration
  - (**Planning**): 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
  - (**Personnel Sec.**): Percentage of individuals screened before being granted access to organizational information and information systems
  - (**System & Service Acquisition**): Percentage of system and service acquisition contracts that include security requirements and/or specifications

Example Candidate Measurements

- **Implementation**
  - (**System & Comm. Protection**): Percentage of mobile computers and devices that perform all cryptographic operations using organizationally specified cryptographic modules operating in approved modes of operations
  - (**System & Info Integrity**): Percentage of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated
- **Effectiveness/**Efficiency
  - (**Access Control**): Percentage of remote access points used to gain unauthorized access
  - (**Certification, Accreditation & Assessment**): Percentage of new systems that have completed certification and accreditation prior to their implementation

Example Candidate Measurements

- **Effectiveness/**Efficiency
  - (**Contingency Planning**): Percentage of information systems that have conducted annual contingency plan testing
  - (**Identification & Authorization**): Percentage of users with access to shared accounts
  - (**Incident Response**): Percentage of incidents reported within required time frame per applicable incident category
  - (**Media Protection**): Percentage of media that passes sanitization procedures testing
  - (**Physical & Environmental**): Percentage of physical security incidents allowing unauthorized entry into facilities containing information assets

Example Candidate Measurements

- Effectiveness**/Efficiency**
  - (**Vulnerability**): Percentage of high vulnerabilities mitigated within organizationally defined time periods after discovery
  - (**Audit & Accountability**): Average frequency of audit records review and analysis for inappropriate activity
  - (**Maintenance**): Percentage of system components that undergo maintenance in accordance with formal maintenance schedules
  - (**Risk Assessment**): Percentage of vulnerabilities remediated within organization-specified time frames
- **Impact**
  - (**Security Budget**): Percentage of the organization's information systems budget devoted to information security

Specifying Measurements

- A critical task in measurement process is to assess and quantify what will be measured
  - collect measurements about **production** from production statistics: effort for completing depends on
    - # of systems
    - # of users of the systems
    - Or more detailed measurement: # of new users, # of access control violations, # of awareness briefings, # of systems by type, # of incidents by category, …
  - collect measurements about **project activities**
    - man hours, resources consumed, outcome in term of loss control or risk reduction, …

Measurements Development

- Design the collecting process
  - "How, when, where, and who"
- Measurements Development Approach
  - Micro-focus measurements
    - examine the performance of an individual control or group of controls within the InfoSec program
  - Macro-focus measurements
    - examine the performance of the overall security program
  - Driven by organization needs and tied to InfoSec goals and objectives

Measurements Development

- Measurement Prioritization and Selection
  - Prioritize metrics in the same manner as the process that they measure
    - facilitate high-priority security controls
    - data obtainability, existence of measurements
  - Use low/medium/high ranking scale, or a weighted scale
- Establish Performance Targets
  - define success in the security program
    - a high percentage (such as 100%) goal
    - Or subjective goals for relative efficiency/effectiveness
  - many InfoSec performance measurements targets are represented by a 100 percent target goal

Measurements Development

- **Measurements Development Template**
  - To document performance measurements in a standardized format
  - To ensure the repeatability of the measurement development, customization, collection, and reporting activities
  - Custom templates can be developed
  - Read Table 7-2 on page 262, and “candidate measures”

Implementing PM

- **Phase 1**: Identify, define, develop, and select InfoSec measures
- **Phase 2**: Consolidate data, identify causes of poor performance
- **Phase 3**: Develop a plan for closing the gap – corrective actions
- **Phase 4**: Develop the business case and **Phase 5**: Obtain resources – Address the budgeting cycle for acquiring resources
- **Phase 6**: Apply corrective actions

Reporting PM

- Make decisions about how to present
  - include the context – list measurements
  - present correlated metrics
    - use pie, line, scatter, or bar charts
    - use colors to denote which kinds of results
- CISO must consider to whom the results should be disseminated and how they should be delivered

TOPIC 7.3 TRENDS IN CERTIFICATION & ACCREDITATION

Certification & Accreditation

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

Emerging Trends in C&A

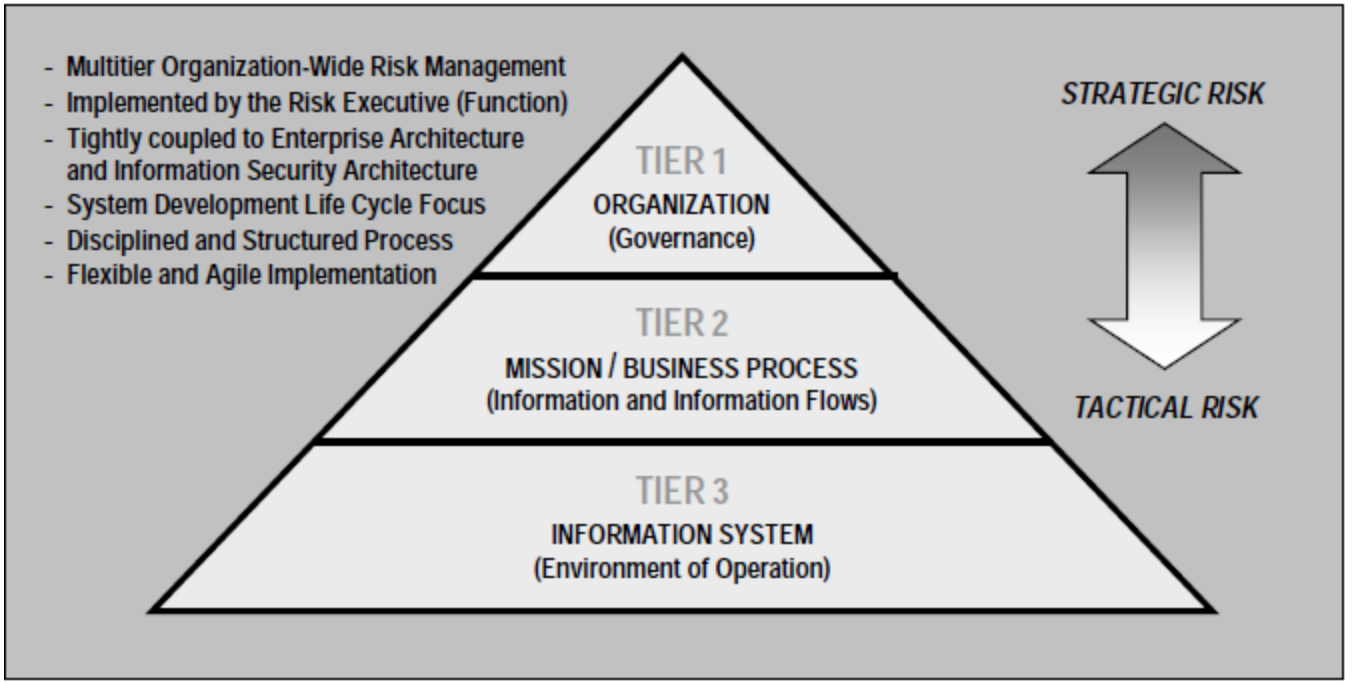
- **NIST SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach**
  - NIST, DoD, ODNI, and CNSS developed the InfoSec framework for the federal government and contractors
  - shift to a process of risk management based assessment and authorization
  - a common approach to a 6-step **Risk Management Framework (RMF)** for InfoSec practice became the standard for the U.S. government

RMF C & A

- The RMF approach is a continuous-improvement method
  - Integrates a lifecycle to C & A
  - C & A are not permanent
    - most accreditation and certification processes require reaccreditation or recertification every few years
  - Offers long-term security

Three-tiered Risk Management

- Most organizations work from the top down
  - focus first on aspects affecting the entire organization
  - move to tactical issues in business processes at tier 2
  - address the most detailed aspects in tier 3



Emerging Trends in C&A

- **SP 800-53 Rev.4: Security and Privacy Controls for Federal Information Systems and Organizations**
  - establish a set of standardized, minimum security controls for IT systems addressing low, moderate, and high levels of concern for confidentiality, integrity, and availability
  - controls are broken into three classes
    - Management
    - Operational
    - Technical

Security Controls

TABLE 1: SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

Security Control Example

AU-2 AUDITABLE EVENTS

Control: The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*].

Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization

Control Enhancements:

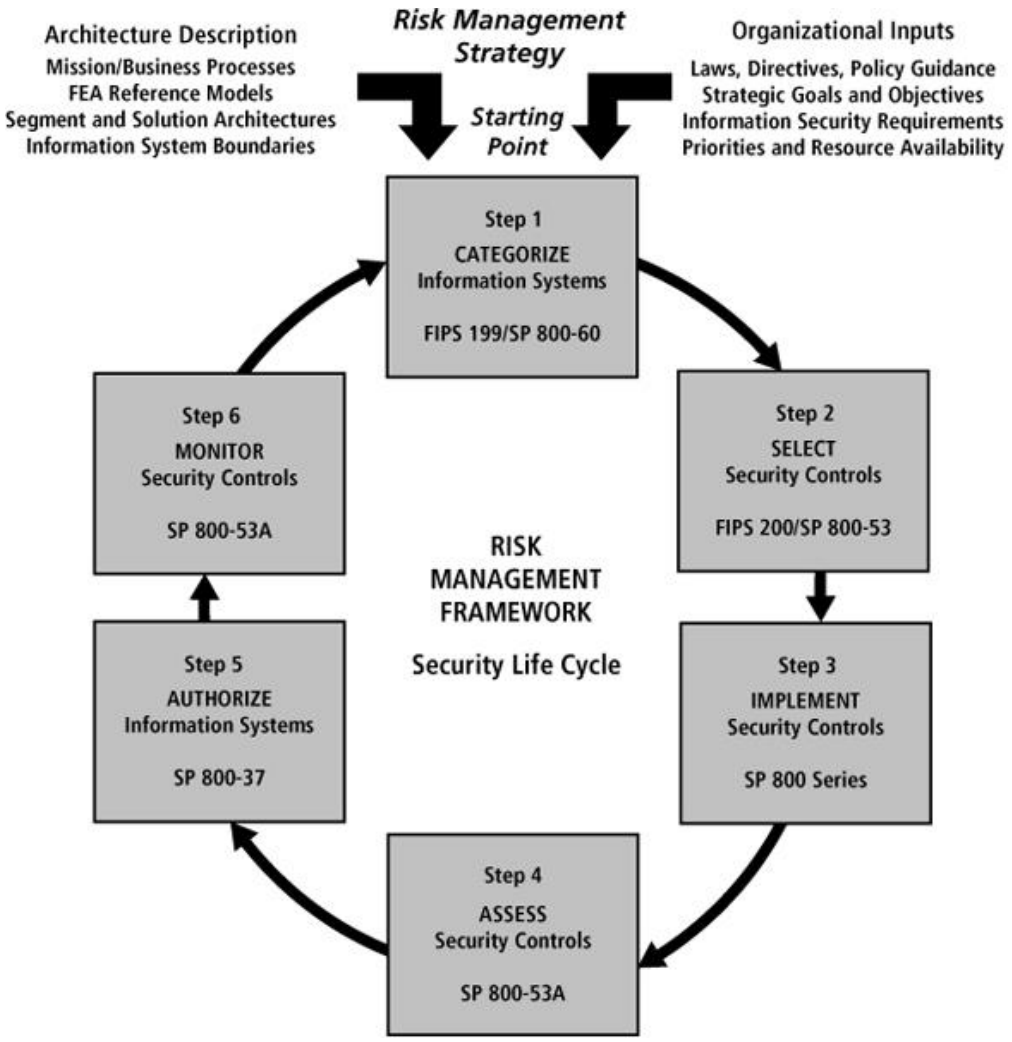
(1) The information system provides the capability to compile audit records from multiple components throughout the system into a systemwide (logical or physical), time-correlated audit trail.

(2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.

(3) The organization periodically reviews and updates the list of organization-defined auditable events.

LOW AU-2	**MOD** AU-2 (3)	**HIGH** AU-2 (1) (2) (3)

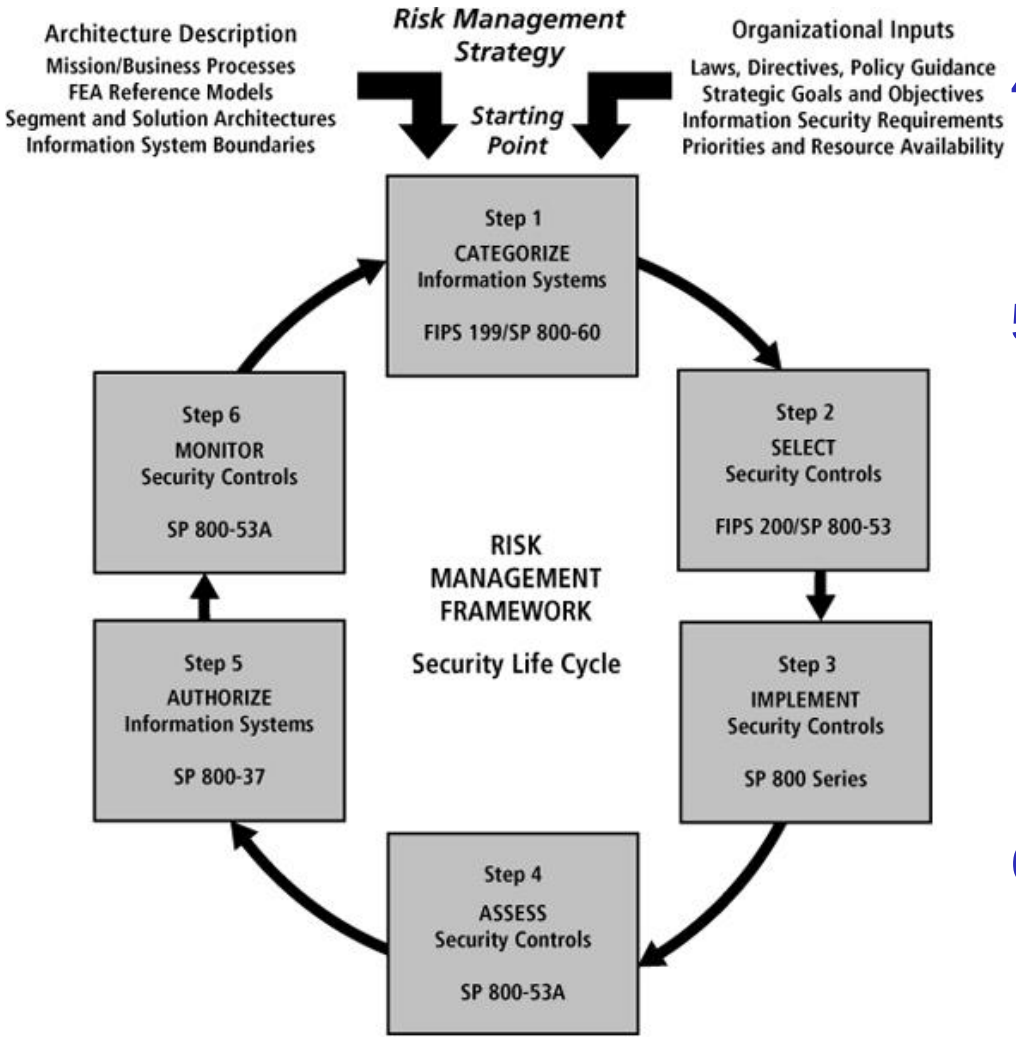
RMF Six-step Process



Initiation:

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

RMF Six-step Process



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
   - Issuance of an authorization decision document becomes C&A

6. Monitor the security controls in the information system on an ongoing basis