

# TEL2813/IS2621

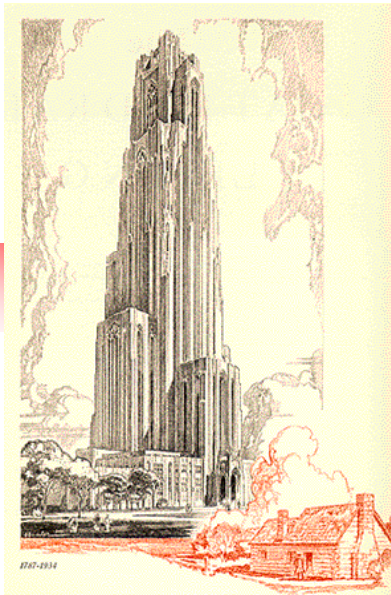
## Security Management

James Joshi

Associate Professor

Lecture 5

Feb 19, 2015



Security Management Models/Practices  
Certification/Accreditation



# Objectives

---

- Overview basic standards and best practices
  - Overview of ISO 27002, COBOT, COSO
  - Overview of NIST SP documents related to security management practices and guidelines, certification and accreditation

Acknowledgement: Whitmann's book (4<sup>th</sup> edition) and slides



# ISO 27002

---

- One of the most widely referenced and often discussed security models
  - BS 7799:1 Information Technology – Code of Practice for Information Security Management,
    - Originally as British Standard BS 7799
    - Now ISO/IEC 17799 (since 2000)
  - It was revised in 2005 and in 2007 was renamed ISO 27002
- The purpose
  - give recommendations for **information security management** for use by those who are responsible for initiating, implementing or maintaining security in their organization

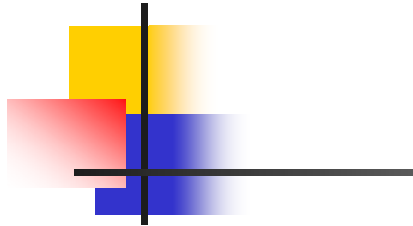


# Sections of ISO/IEC 27002

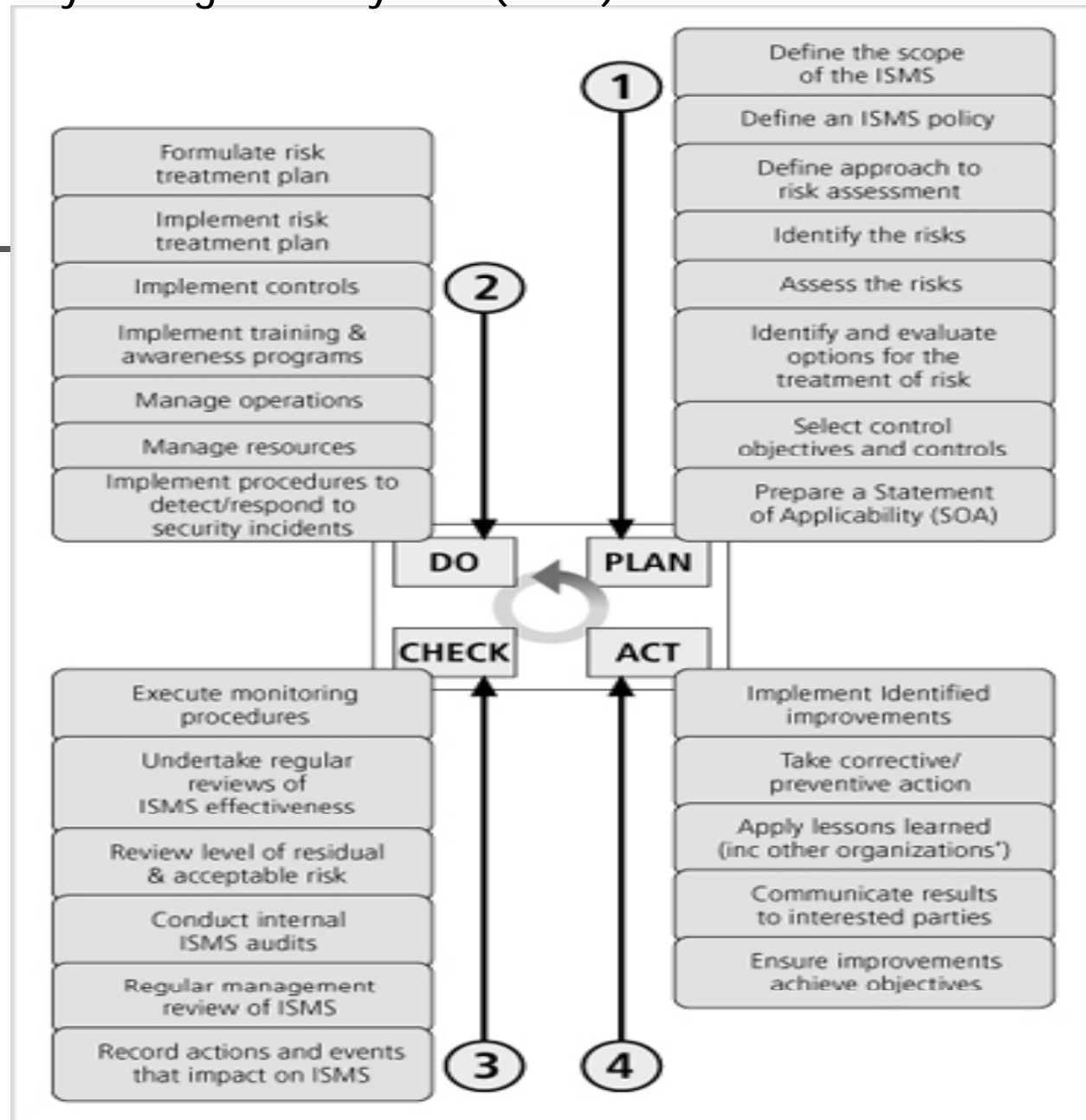
---

- Structure
- Risk Assessment and Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resource Security
- Physical and Environmental Security
- Communications and Operations
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

# Information Security Management System (ISMS)



ISO/IEC 27001  
major process  
steps





# RFC 2196 Site Security Handbook

---

- RFC 2196
  - Created by the Security Area Working Group within the IETF
  - provides a good **functional discussion of important security issues** along with *development* and *implementation* details
  - Covers
    - security policies, security technical architecture, security services, and security incident handling
  - **HIGHLIGHTS:** importance of security policies, examination of services, access controls, etc.



# NIST Security Models

---

- NIST documents have two notable advantages:
  - Publicly available at no charge
  - Have been broadly reviewed by government and industry professionals
    - SP 800-12, Computer Security Handbook
    - SP 800-14, Generally Accepted Security Principles & Practices
    - SP 800-18, Guide for Developing Security Plans
    - SP 800-26, Security Self-Assessment Guide-IT Systems
    - SP 800-30, Risk Management for Information Technology Systems



# NIST SP 800-12

## The Computer Security Handbook

---

- Excellent reference and guide for *routine management of information security*
  - Little on design and implementation
- Lays out NIST philosophy on security management by identifying **17 controls** organized into three categories:
  - Management Controls section
    - addresses security topics characterized as managerial
  - Operational Controls section
    - addresses security controls focused on controls that are, broadly speaking, **implemented and executed by people**
  - Technical Controls section
    - focuses on security controls that the computer system executes





# NIST Special Publication 800-14

Generally Accepted Principles and Practices for Securing  
Information Technology Systems

---

- Describes best practices useful in the development of a security blueprint
- Describes principles that should be integrated into information security processes
- Documents 8 points and 33 Principles



# NIST Special Publication 800-14

## Key Points

---

- Key points made in NIST SP 800-14 are:
  - Security Supports the Mission of the Organization
  - Security is an Integral Element of Sound Management
    - Planning, organizing, leading & controlling activities
  - Security Should Be Cost-Effective
  - Systems Owners Have Security Responsibilities Outside Their Own Organizations (*all stakeholders*)
  - Security Responsibilities and Accountability Should Be Made Explicit
  - Security Requires a Comprehensive and Integrated Approach
    - SecSDLC, communities of interest
  - Security Should Be Periodically Reassessed
  - Security is Constrained by Societal Factors

# NIST Special Publication 800-18

## A Guide for Developing Security Plans for Information Technology Systems

---

- Provides
  - detailed methods for *assessing*, *designing*, and *implementing* controls and plans for various sized applications
- Serves as a guide for the activities
  - for the overall *information security planning process*
- Includes templates for major application security plans

# NIST Special Publication 800-26

## 17 areas Defining the core of the NIST Security Management Structure

### ■ Management Controls

1. Risk Management
2. Review of Security Controls
3. Life Cycle Maintenance
4. Authorization of Processing  
(Certification and Accreditation)
5. System Security Plan

### ■ Operational Controls

6. Personnel Security
7. Physical Security
8. Production, Input/Output Controls
9. Contingency Planning
10. Hardware and Systems Software
11. Data Integrity
12. Documentation
13. Security Awareness, Training, and Education
14. Incident Response Capability

### ■ Technical Controls

15. Identification and Authentication
16. Logical Access Controls
17. Audit Trails



# Hybrid Security Management Model

---

## ■ Management controls

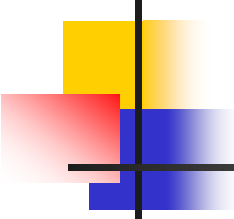
- Program management
- System security plan
- Life cycle management
- Risk management
- Review of security controls
- Legal compliance

## ■ Operational controls

- Contingency planning
- Security education, training and awareness
- Personnel security
- Physical security
- Production inputs and outputs
- Hardware and software systems maintenance
- Data integrity

## ■ Technical controls

- Logical access controls
- Identification, authentication, authorization and accountability
- Audit trails
- Asset classification and control
- cryptography



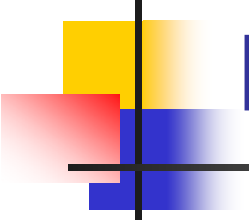
# NIST Special Publication 800-30

## Risk Management Guide for Information Technology Systems

---

- Provides a foundation for the development of an effective risk management program
- Contains both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems
- Strives to enable organizations to better manage IT-related risks

Risk Management Overview
Risk Assessment
Risk Mitigation
Evaluation and Assessment

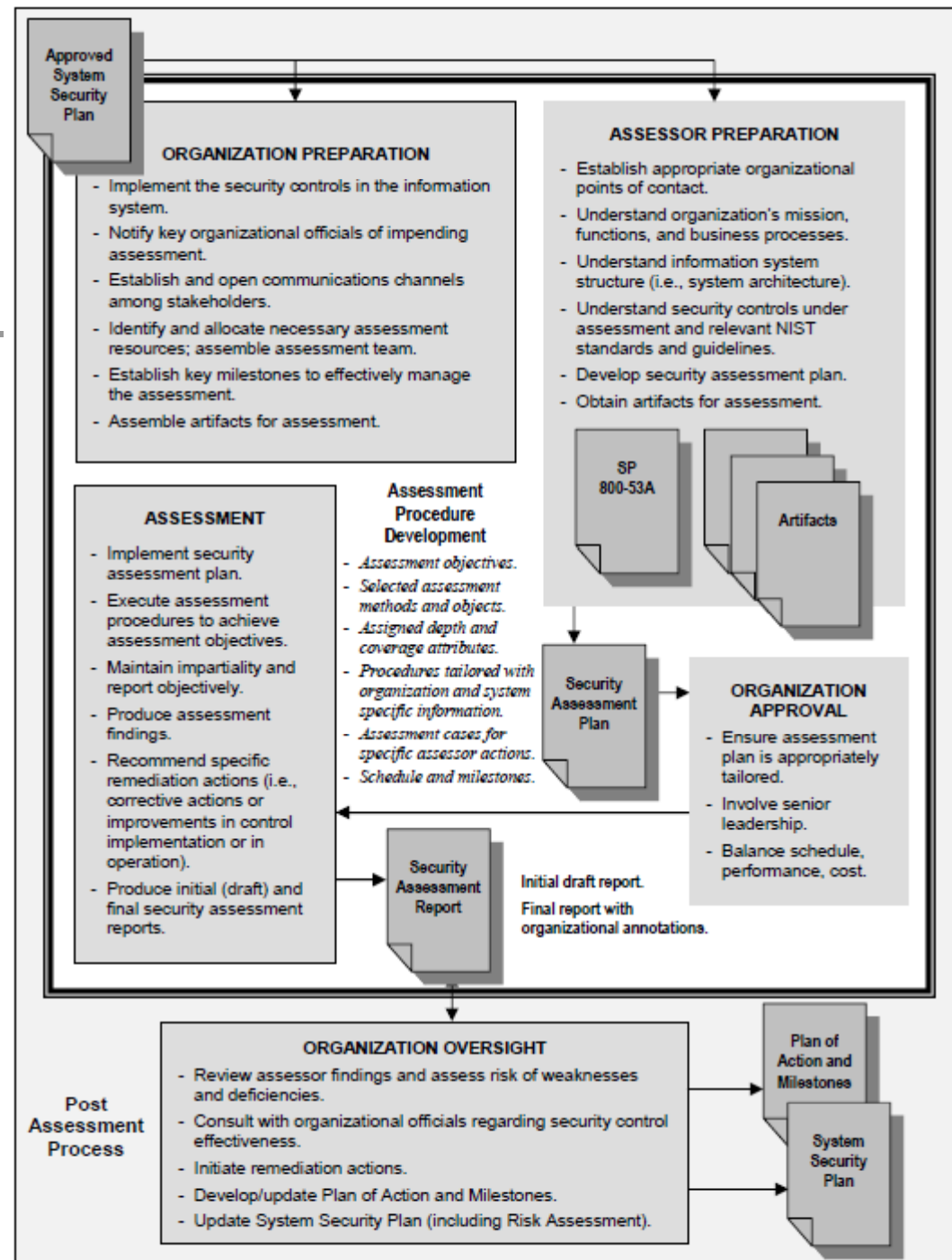


# NIST Special Publications 800-53 Rev. 3 and 800-53A Rev. 1

---

- Both publications cover *recommended security controls for Federal Information Systems*
- SP 800-53, Revision 3 provides a systems development life cycle (SDLC) approach to security assessment of information systems
- NIST has a **comprehensive security control assessment program** that guides organizations through the:
  - *Preparation for, assessment of, and remediation of* critical security controls
- More recent is Rev 4!

# NIST Security Control Assessment process Overview







# COBIT

## Governance

ensures that enterprise objectives are achieved by (EDM)

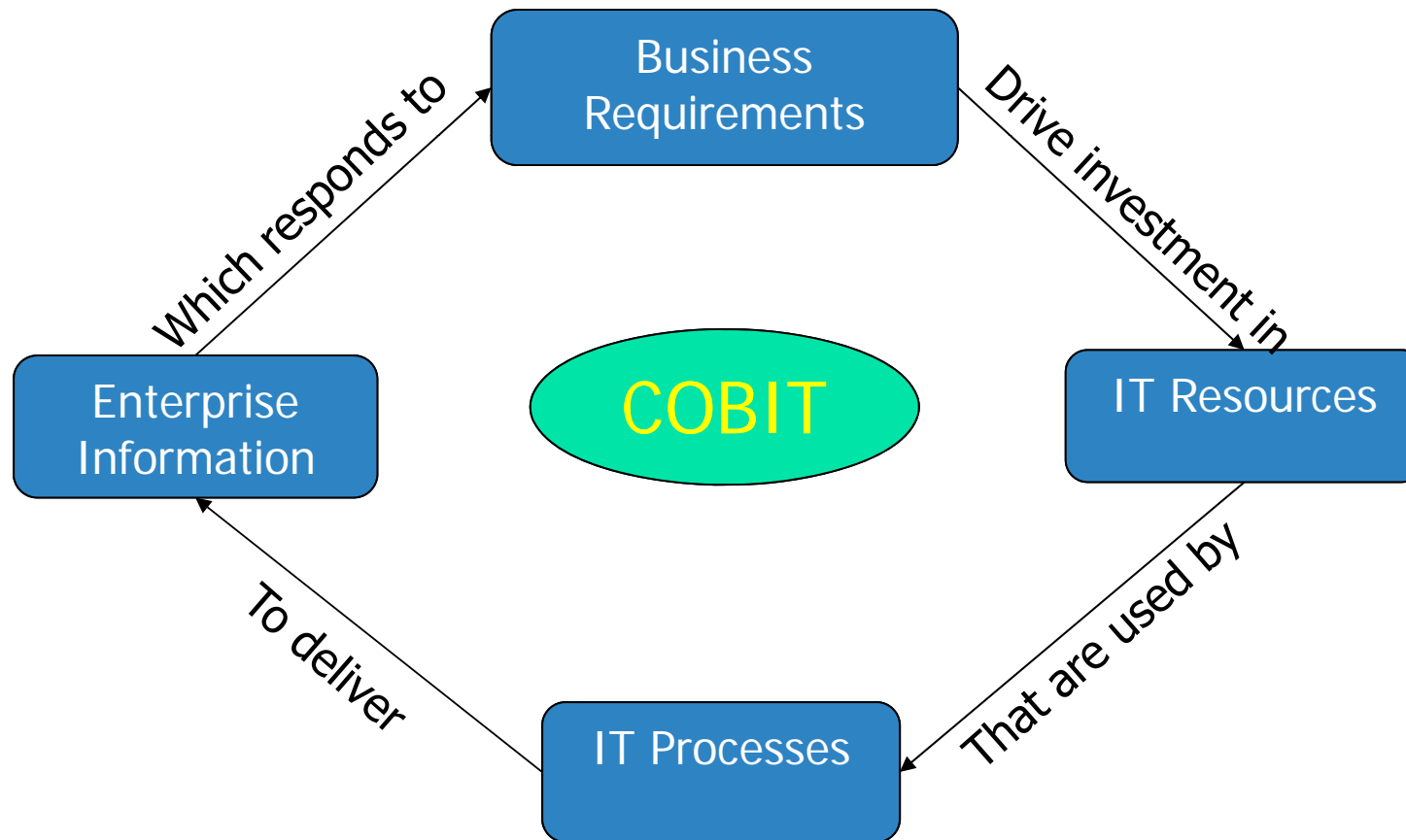
*-Evaluation, Direction, Monitoring.*

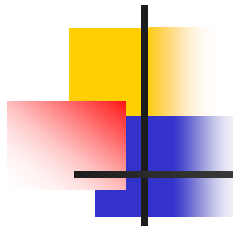
## Management (PBRM)

*-Plans, Builds, Runs and Monitors.*

- “*Control Objectives for Information and Related Technology*” (COBIT)
  - Provides advice about the implementation of sound controls and control objectives for InfoSec
- COBIT was created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992
  - There have been many updates
  - Latest version is COBIT 5 released in 2012

# Basic COBIT Principle





# COBIT

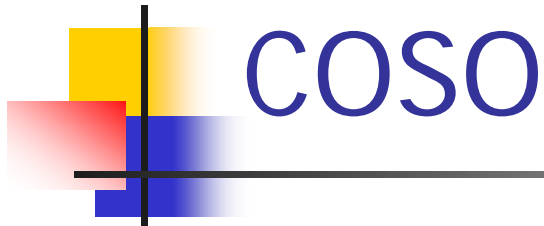
---

- COBIT 5 provides five principles focused on the governance and management of IT:
  - *Meeting Stakeholder Needs*
  - *Covering the Enterprise End-to-End*
  - *Applying a Single, Integrated Framework*
  - *Enabling a Holistic Approach*
  - *Separating Governance from Management*
- 4 IT (process oriented) domains and 34 IT processes
  - Plan and Organize
  - Acquire and Implement
  - Deliver and Support
  - Monitor and Evaluate

## Enablers

1. Principles, policies and frameworks
2. Processes
3. Organizational structures
4. Culture, ethics and behavior
5. Information
6. Services, infrastructure and applications
7. People, skills and competencies

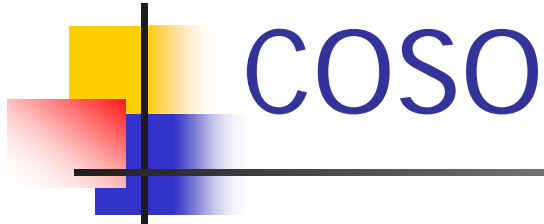
- Designed more for IT governance structure
- Also provides framework to support infoSec requirements and assessment needs



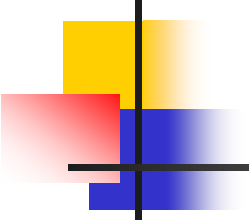
- Committee of Sponsoring Organizations (COSO) of the Treadway Commission (private sector)
  - Another control-based model
- Major objective:
  - identify the factors that cause **fraudulent financial reporting** and to make recommendations to reduce its incidence
- COSO helps organizations comply with critical regulations
  - E.g., Sarbanes-Oxley Act of 2002



- According to COSO
  - internal control is a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories::
    - *Effectiveness and efficiency of operations*
    - *Reliability of financial reporting*
    - *Compliance with applicable laws and regulations*



- The COSO framework is built on five interrelated components:
  - Control environment (for internal controls)
    - Environmental factors: integrity, ethics/culture, operating styles
  - Risk assessment
  - Control activities
    - Policies and procedures for mgmt directives (approvals, authorizations, segregation duties ...)
  - Information and communication
  - Monitoring



# Information Technology Infrastructure Library

---

- Information Technology Infrastructure Library (ITIL)
  - A collection of methods and practices for managing the development and operation of IT infrastructures
- ITIL has produced a series of books
  - Each of which covers an IT management topic
- Since ITIL includes a detailed description of many significant IT-related practices
  - It can be tailored to many IT organizations



# Information Security Governance Framework (ISGF)

---

- The ISGF is a managerial model provided by an industry working group
  - National Cyber Security Partnership (industry WG)
- The framework
  - provides guidance in the development and implementations of an organizational InfoSec governance structure
  - also specifies that each independent organizational unit should develop, document, and implement in InfoSec program consistent with accepted security practices
  - Recommends responsibilities of various personnel
    - BoD/BoT, Senior Executives, Executive team, Senior Manager, All employees and users





# Security Management Practices

---

- In information security, two categories of benchmarks are used
  - Standards of due care/due diligence
  - Best practices
- Gold standard – subcategory of Best practices
  - regarded as “the best of the best”



# Standards of Due Care/ Diligence

---

- Standard of due care
  - adopt minimum levels of security for a **legal defense**,
    - they may need to show that they have done what any prudent organization would do in similar circumstances
- Due diligence
  - Demonstrated by implementing controls at **this minimum standard**, and maintaining them
  - Requires that an organization ensure that the implemented standards **continue to provide** the required level of protection
  - Failure to support a standard of due care or due diligence
    - can expose an organization to legal liability,
    - provided it can be shown that the organization was negligent in its application or lack of application of information protection



# Best Security Practices

---

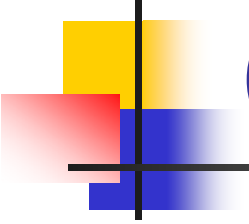
- Best business practices or simply best practices
  - Security efforts that seek to provide a superior level of performance in the protection of information
  - Some organizations call them recommended practices
- Best security practices
  - Security efforts that are among the best in the industry
    - Balanced
    - Defense in depth
- Companies with best practices may not be the best in every area



# Recommended Security Practices

---

- 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)
- 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 shows Federal agency BSPs*



# VISA International Security Model (best practices example)

---

- VISA uses two important documents that improve and regulate its information systems:
  - Security Assessment Process document
    - contains series of recommendations for detailed examination of organization's systems with the eventual goal of integration into the VISA systems
  - Agreed Upon Procedures document
    - outlines the policies and technologies used to safeguard security systems that carry the sensitive cardholder information to and from VISA systems



# The Gold Standard

---

- A model level of performance
  - Demonstrates industrial leadership, quality, and concern for the protection of information
- The implementation of gold standard security requires
  - a great deal of support, both in financial and personnel resources
- No published criteria!



# Selecting Best Practices

---

- Choosing recommended practices could be a challenge
  - In industries that are regulated by governmental agencies,
    - government guidelines are often requirements
  - For other organizations,
    - government guidelines are excellent sources of information and can inform their selection of best practices



# Selecting Best Practices (Continued)

---

- When considering best practices for your organization, consider the following:
  - 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?





# Best Practices

---

- Microsoft best practices (at its Web site)
  - Use antivirus software
  - Use strong passwords
  - Verify your software security settings
  - Update product security
  - Build personal firewalls
  - Back up early and often
  - Protect against power surges and loss



# Benchmarking and Best Practices Limitations

---

- Biggest problems with benchmarking in information security:
  - Organizations don't talk to each other and are not identical
    - Successful attack is viewed as organizational failure and is kept secret, insofar as possible
      - Join professional associations and societies like ISSA and sharing their stories and lessons learned
    - Alternative to this direct dialogue is the publication of lessons learned
  - No two organizations are identical
  - Best practices are moving targets



# Baselining

---

- Baseline:
  - “value or profile of a performance metric against which changes in the performance metric can be usefully compared”
- Baselining:
  - process of measuring against established standards
  - In InfoSec,
    - the comparison of security activities and events against the organization’s future performance
  - Can provide foundation for internal benchmarking, as information gathered for an organization’s first risk assessment becomes the baseline for future comparisons



# Performance Measurement in InfoSec Management

---

- Benefits and performance of InfoSec are measurable
  - requires the design and ongoing use of an InfoSec performance management program
  - Need effective performance metrics



# 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 /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

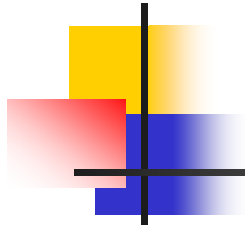


# InfoSec Performance Management

---

- 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



# Information Security Metrics

---

- Before designing, collecting, and using measurements, the CISO should answer:
  - 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?



# Building the Performance Measurement Program

---

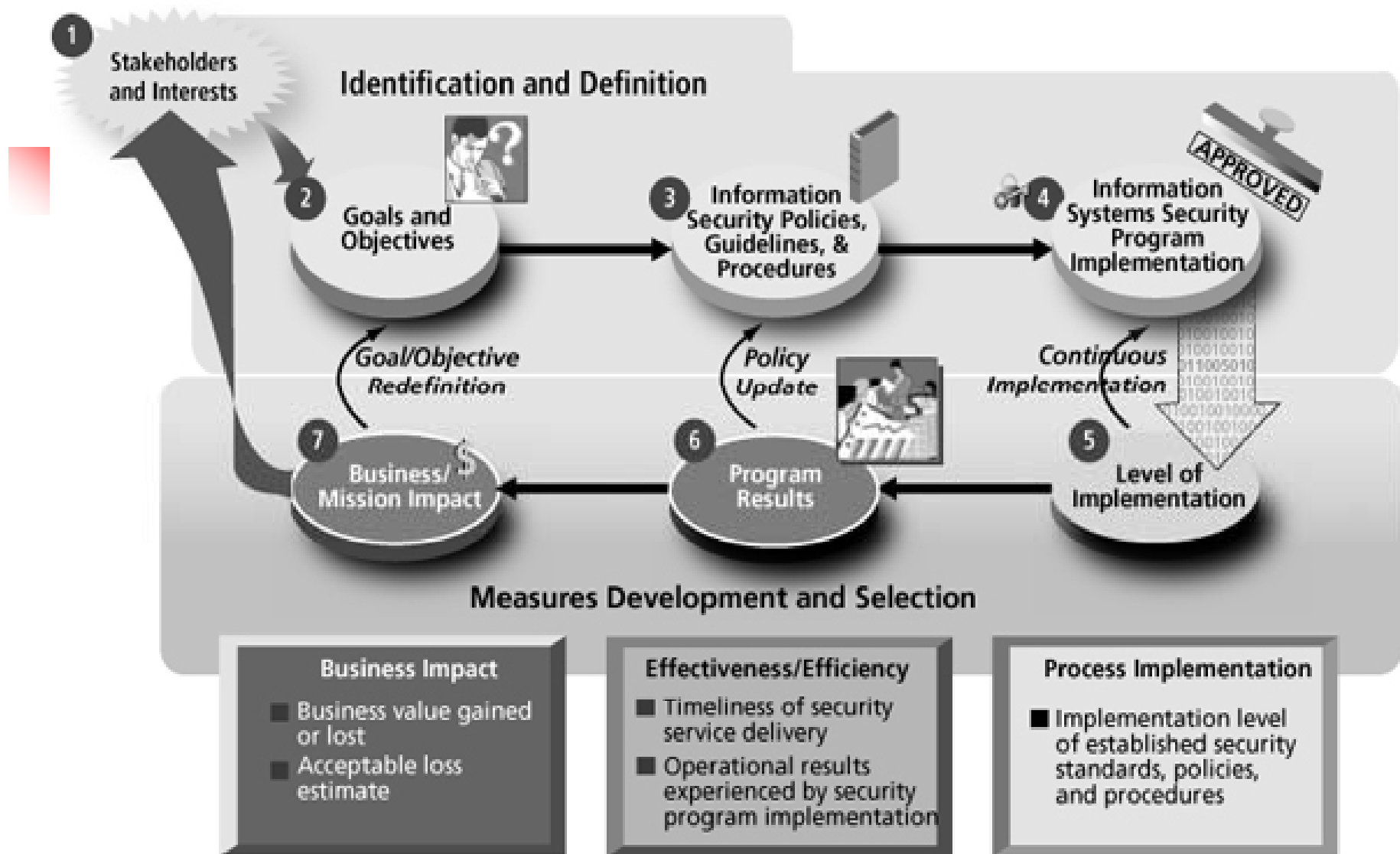
- PM should demonstrate value to the organization
- Benefits of using InfoSec PM:
  - Increasing accountability for InfoSec performance
  - Improving effectiveness of InfoSec activities
  - Demonstrating compliance with laws, rules, and regulations
  - Providing quantifiable inputs for resource allocation 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



**Figure 7-1** 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

*Instructions for the development and format of such template are provided in Table 7-2 starting on page 262*

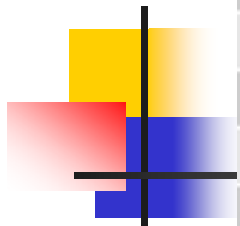


# Collecting InfoSec Measurements

---

- **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”



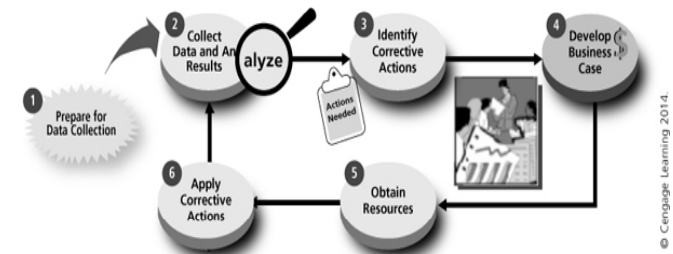
Percentage of the organization's information systems budget devoted to InfoSec
Percentage of high vulnerabilities mitigated within organizationally defined time periods after discovery
Percentage space of remote access points used to gain unauthorized access
Percentage of information systems personnel 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 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 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

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

**Table 7-4** Examples of possible security performance measurements

# 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
  - *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





# 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



# Emerging Trends In Certification And Accreditation

---

- Accreditation

- is authorization of an IT system to process, store, or transmit information
  - Issued by management official
  - Serves as means of assuring that systems are of adequate quality
  - Also challenges managers and technical staff to find best methods to assure security, given technical constraints, operational constraints, and mission requirements



# Emerging Trends In Certification And Accreditation (Continued)

---

- Certification:
  - “the comprehensive evaluation of the technical and non-technical security controls of an IT system to support the accreditation process that establishes the extent to which 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 customers



# SP 800-37

## Guidelines for the Security Certification and Accreditation of Federal IT Systems

---

- Three project goals
  - Develop standard guidelines and procedures for certifying and accrediting federal IT systems including critical infrastructure of United States
  - Define essential minimum security controls for federal IT systems
  - Promote
    - development of public and private sector assessment organizations and
    - certification of individuals capable of providing cost effective, high quality, security certifications based on standard guidelines and procedures

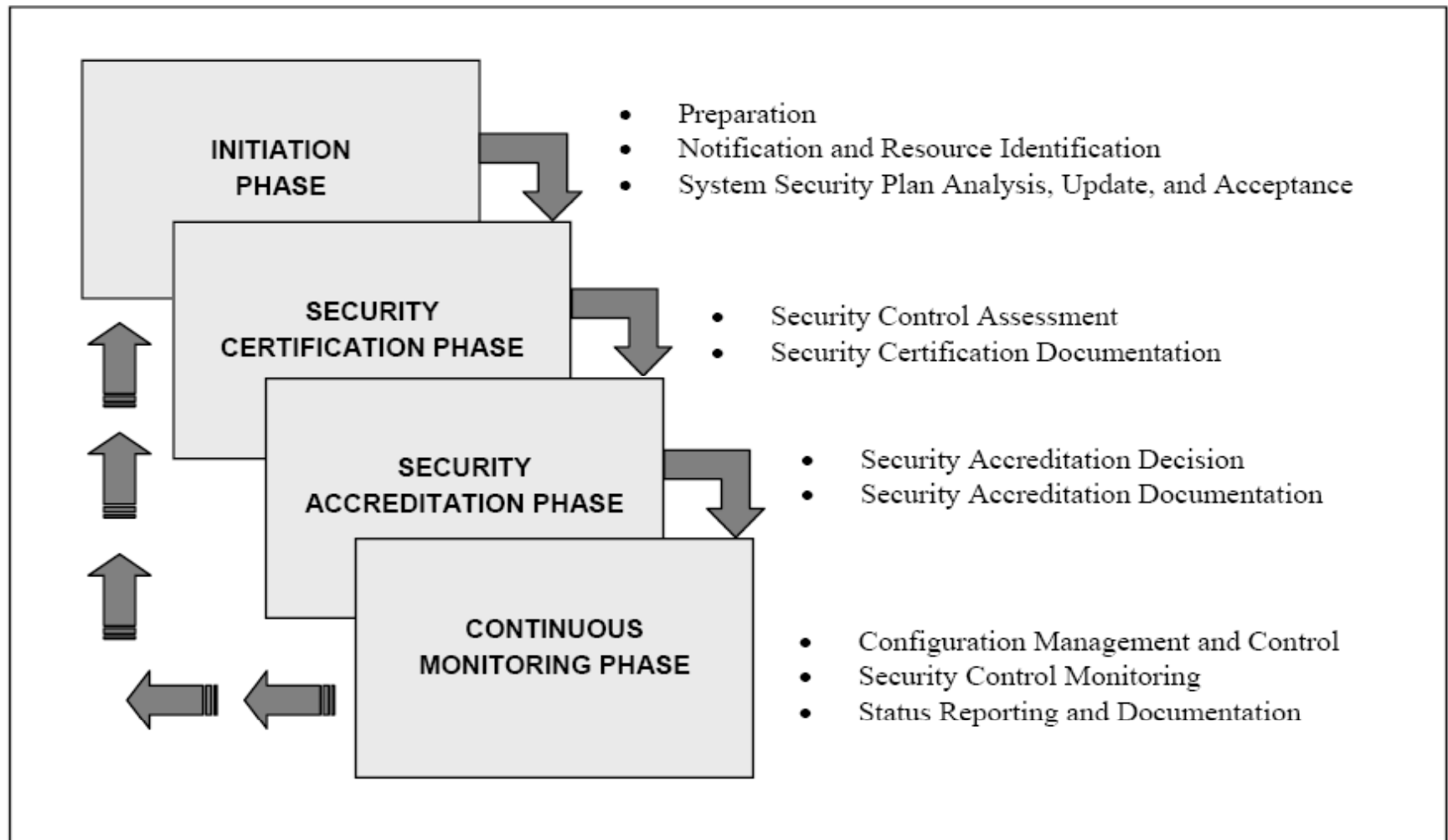
# SP 800-37 (Continued)

## Guidelines for the Security Certification and Accreditation of Federal IT Systems

---

- Specific benefits of security certification and accreditation (C&A) initiative include:
  - More consistent, comparable, and repeatable certifications of IT systems
  - More complete, reliable, information for **authorizing officials**—leading to better understanding of complex IT systems and associated risks and vulnerabilities—and therefore, more informed decisions by management officials
  - Greater availability of competent security evaluation and assessment services
  - More secure IT systems within the federal government”

# The Process





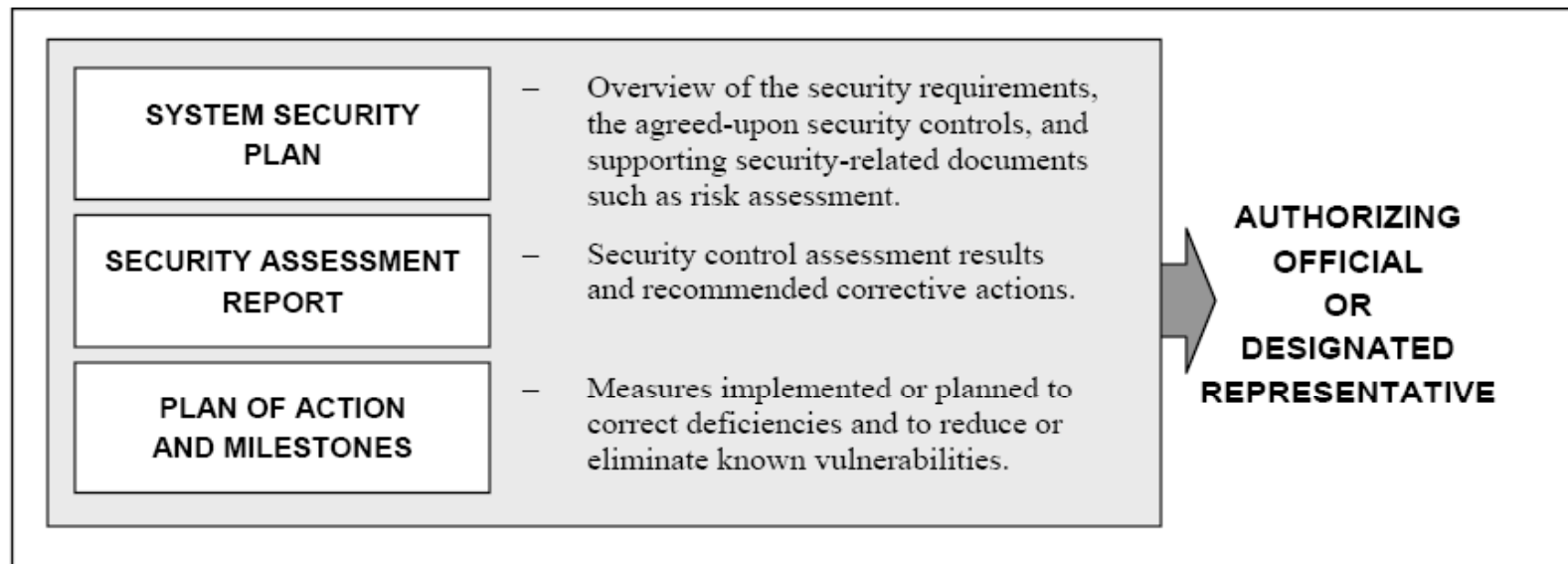


# Planned Federal System Certifications

---

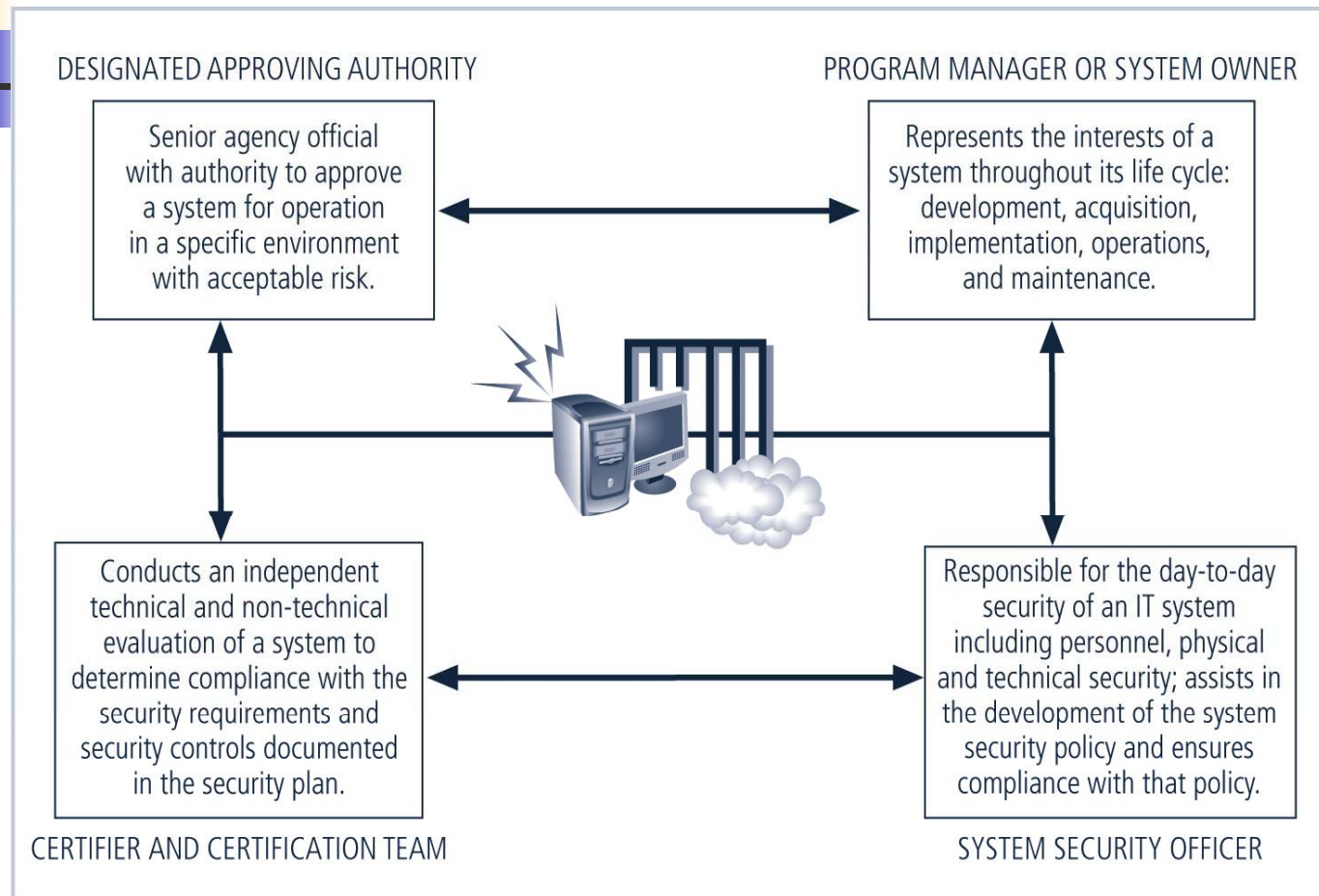
- Systems are to be certified to one of three levels:
  - Security Certification Level 1: Entry-Level Certification  
Appropriate For Low Priority (Concern) Systems
  - Security Certification Level 2: Mid-Level Certification  
Appropriate For Moderate Priority (Concern) Systems
  - Security Certification Level 3: Top-Level Certification  
Appropriate For High Priority (Concern) Systems

# Accreditation Package & Decision



- Decision letter
  - Security accreditation decision letter
    - Authorize to operate - Authorized to operate in interim basis – Not authorized to operate
  - Supporting rationale for the decision
  - Terms and condition for the decision

# Participants in the Federal C&A Process



**FIGURE 6-4** Participants in the Certification and Accreditation Process

# SP 800-53

## Minimum Security Controls for Federal IT Systems

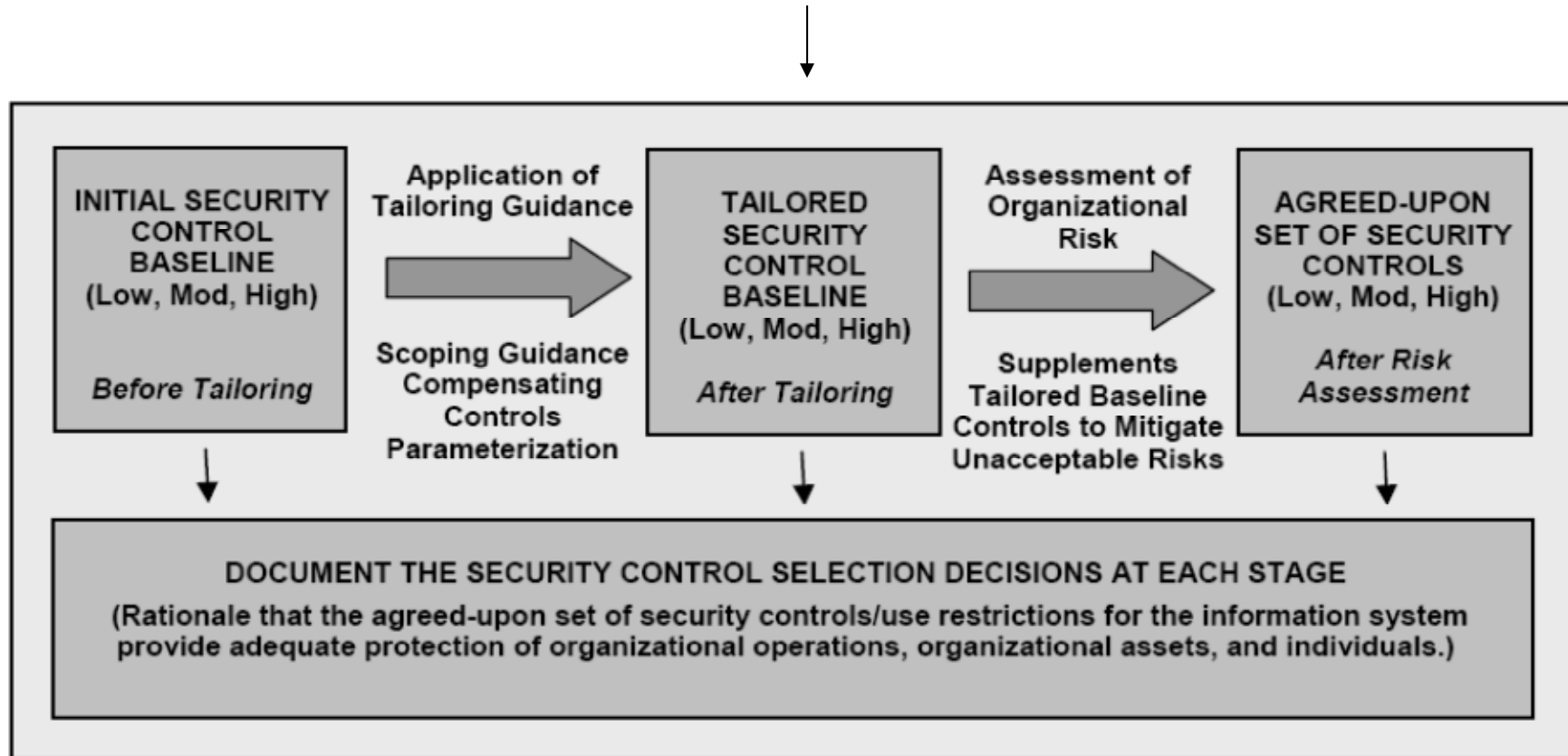
---

- SP 800-53 is part two of the Certification and Accreditation project
- Purpose
  - to 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 the three familiar general classes of security controls
  - management,
  - operational, and
  - technical



# Security Control Selection Process

Risk-Management Framework



**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 Structure (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)
----------	--------------	-----------------------

(Complete catalog is provided at the end of 800-53)



# Summary

---

- Overview of
  - Security management models
  - Security practices
- Certification and accreditation issues