



TEL2813/IS2820

Security Management

Security Management Models And
Practices

Feb 5, 2008



Objectives

- Overview basic standards and best practices
 - Overview of ISO 17799
 - Overview of NIST SP documents related to security management practices and guidelines, certification and accreditation



Introduction

- To create or maintain a secure environment
 1. Design working security plan
 2. Implement management model to execute and maintain the plan
- Basic steps:
 - begin with creation or validation of security framework,
 - followed by an information security blueprint describing existing controls and identifying other necessary security controls



Introduction (Continued)

- Framework:
 - outline of the more thorough blueprint,
 - Blueprint
 - basis for the design, selection, and implementation of all subsequent security controls
- To develop a blueprint or methodology
 - Use established security management models and practices



BS 7799

- 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)
 - BS 7799:2 Information Security Management: Specification with Guidance for Use
- The purpose of ISO/IEC 17799 (BS 7799:1)
 - give recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization



BS 7799 (Continued)

- Volume 2
 - provides information on how to implement Volume 1 (17799) and
 - how to set up an Information Security Management Structure (ISMS)
 - ISMS Certification and accreditation done by BS 7799 certified evaluator
- Standard has not been adopted by US, Germany, Japan etc.



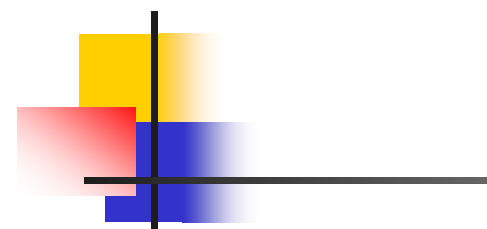
ISO/IEC 17799 Drawbacks

- The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799
- Lacks “the necessary measurement precision of a technical standard”
- No reason to believe that ISO/IEC 17799 is more useful than any other approach
- Not as complete as other frameworks
- Perceived to have been hurriedly prepared, given tremendous impact its adoption could have on industry information security controls

The Ten Sections Of ISO/IEC 17799



1. Organizational Security Policy
2. Organizational Security Infrastructure objectives
3. Asset Classification and Control
4. Personnel Security objectives
5. Physical and Environmental Security objectives
6. Communications and Operations Management objectives
7. System Access Control objectives
8. System Development and Maintenance objectives
9. Business Continuity Planning
10. Compliance objectives



Plan-Do-Check-Act of BS7799:2

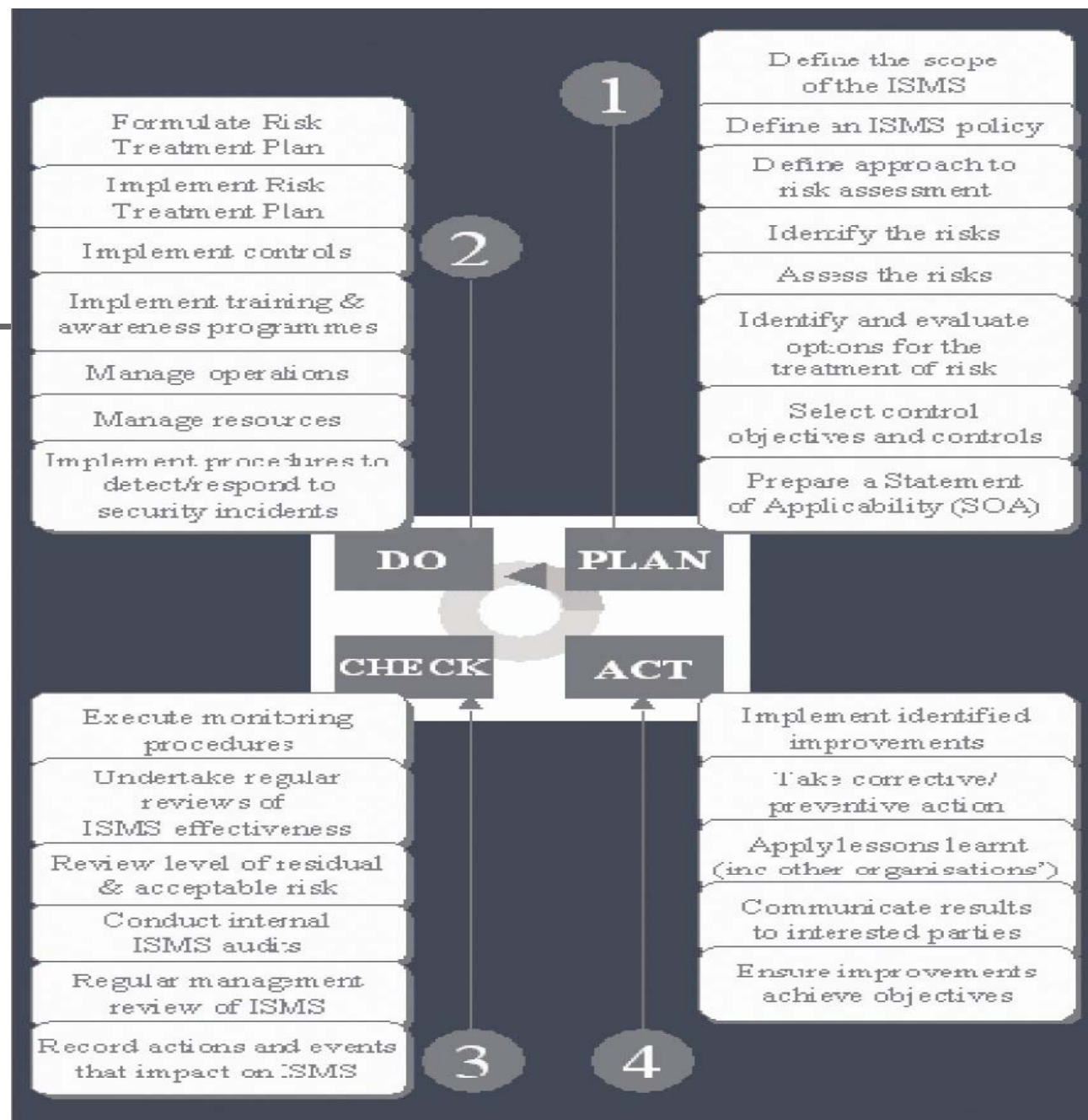


FIGURE 6-2 Plan-Do-Check-Act Cycle from BS 7799:2



The Security Management Index and ISO 17799

- To determine how closely an organization is complying with ISO 17799, take Human Firewall Council's survey, the Security Management Index (SMI)
 - Asks 35 questions over 10 domains of ISO standard
 - Gathers metrics on how organizations manage security
 - Survey has been developed according to ISO 17799 international security standards to reflect best practices from a global perspective
 - Enables information security officers to benchmark their practices against those of other organizations

The Human Firewall Council



SMI

- Familiarize yourself with the 10 categories of security management
- Benchmark your organization's security management practices by taking the survey
- Evaluate your results in each category to identify strengths and weaknesses
- Examine the suggestions for improvement in each category in this report
- Use your SMI results to gain support for improving security



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
 - Also includes discussion of the 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 (as opposed to systems)
 - 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
 - Security Should Be Cost-Effective
 - Systems Owners Have Security Responsibilities Outside Their Own Organizations
 - Security Responsibilities and Accountability Should Be Made Explicit
 - Security Requires a Comprehensive and Integrated Approach
 - Security Should Be Periodically Reassessed
 - Security is Constrained by Societal Factors

NIST Special Publication 800-14

Principles



1. Establish sound security policy as “foundation” for design
2. Treat security as integral part of overall system design
3. Clearly delineate physical and logical security boundaries governed by associated security policies
4. Reduce risk to acceptable level
5. Assume that external systems are insecure
6. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness
7. Implement layered security (Ensure no single point of vulnerability)

Checklist for the
security blueprint



NIST Special Publication 800-14

Principles (Continued)

8. Implement tailored system security measures to meet organizational security goals
9. Strive for simplicity
10. Design and operate an IT system to limit vulnerability and to be resilient in response
11. Minimize system elements to be trusted
12. Implement security through a combination of measures distributed physically and logically
13. Provide assurance that the system is, and continues to be, resilient in the face of expected threats
14. Limit or contain vulnerabilities
15. Formulate security measures to address multiple overlapping information domains
16. Isolate public access systems from mission critical resources
17. Use boundary mechanisms to separate computing systems and network infrastructures
18. Where possible, base security on open standards for portability and interoperability
19. Use common language in developing security requirements.
20. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations



NIST Special Publication 800-14

Principles (Continued)

21. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process
22. Authenticate users and processes to ensure appropriate access control decisions both within and across domains
23. Use unique identities to ensure accountability
24. Implement least privilege
25. Do not implement unnecessary security mechanisms
26. Protect information while being processed, in transit, and in storage
27. Strive for operational ease of use
28. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability
29. Consider custom products to achieve adequate security
30. Ensure proper security in the shutdown or disposal of a system
31. Protect against all likely classes of "attacks"
32. Identify and prevent common errors and vulnerabilities
33. Ensure that developers are trained in how to develop secure software

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

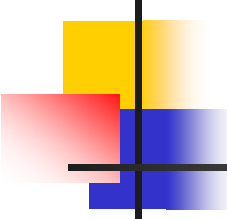
- Program management
- System security plan
- Life cycle management
- Risk management
- Review of security controls
- Legal compliance

■ 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



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
 - that are generally regarded as “the best of the best”



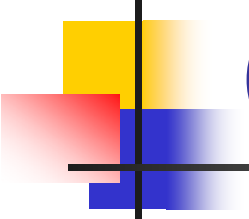
Standards of Due Care/ Diligence

- Standard of due care
 - organizations 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
- Federal Agency Best Security Practices
(<http://csrc.nist.gov/groups/SMA/fasp/areas.html>)



VISA International Security Model (best practices example)

- VISA use 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



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

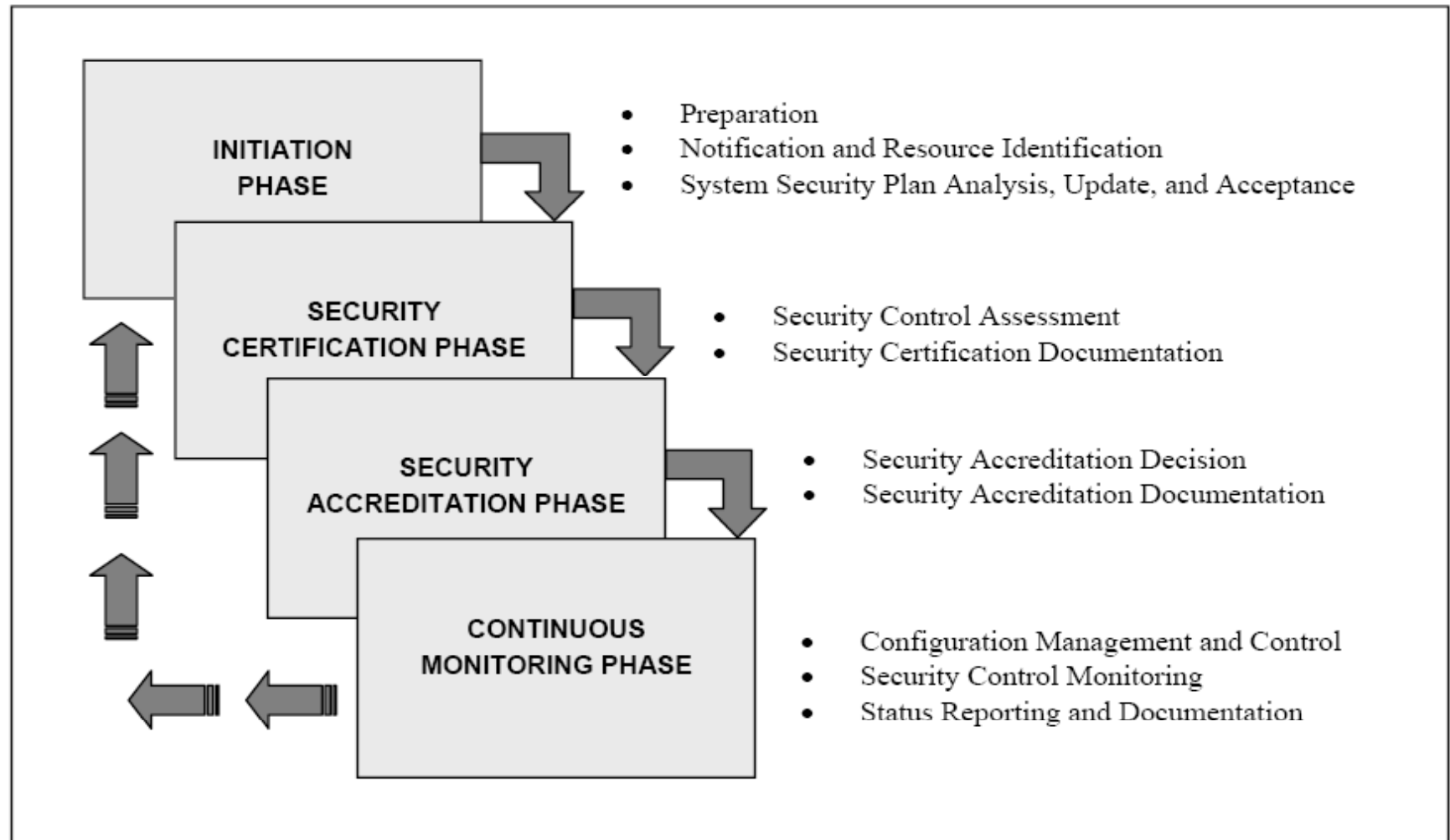
- Three project goals
 - Develop standard guidelines and procedures for certifying and accrediting federal IT systems including critical infrastructure of United States
 - Define essential minimum security controls for federal IT systems
 - Promote
 - development of public and private sector assessment 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



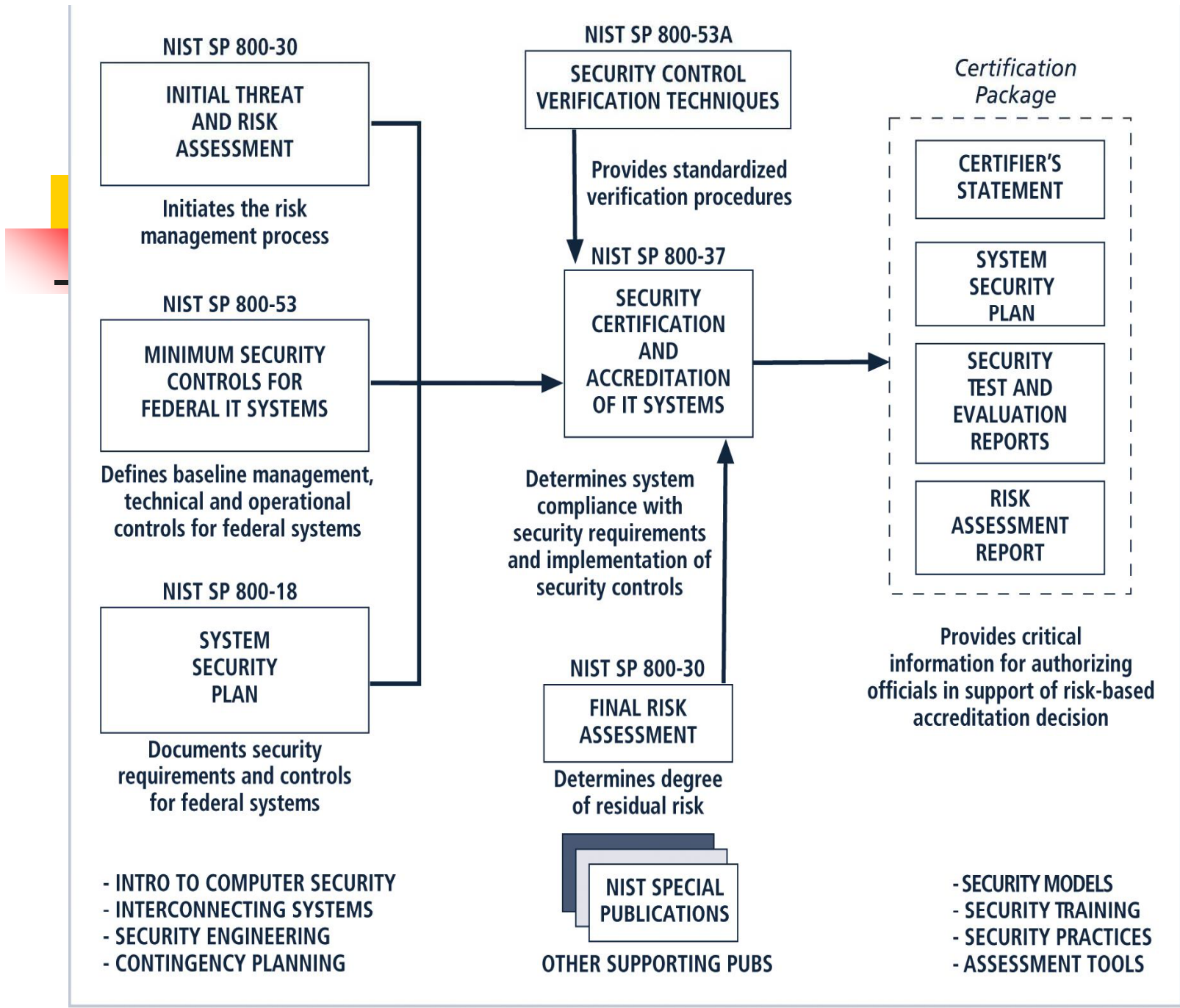


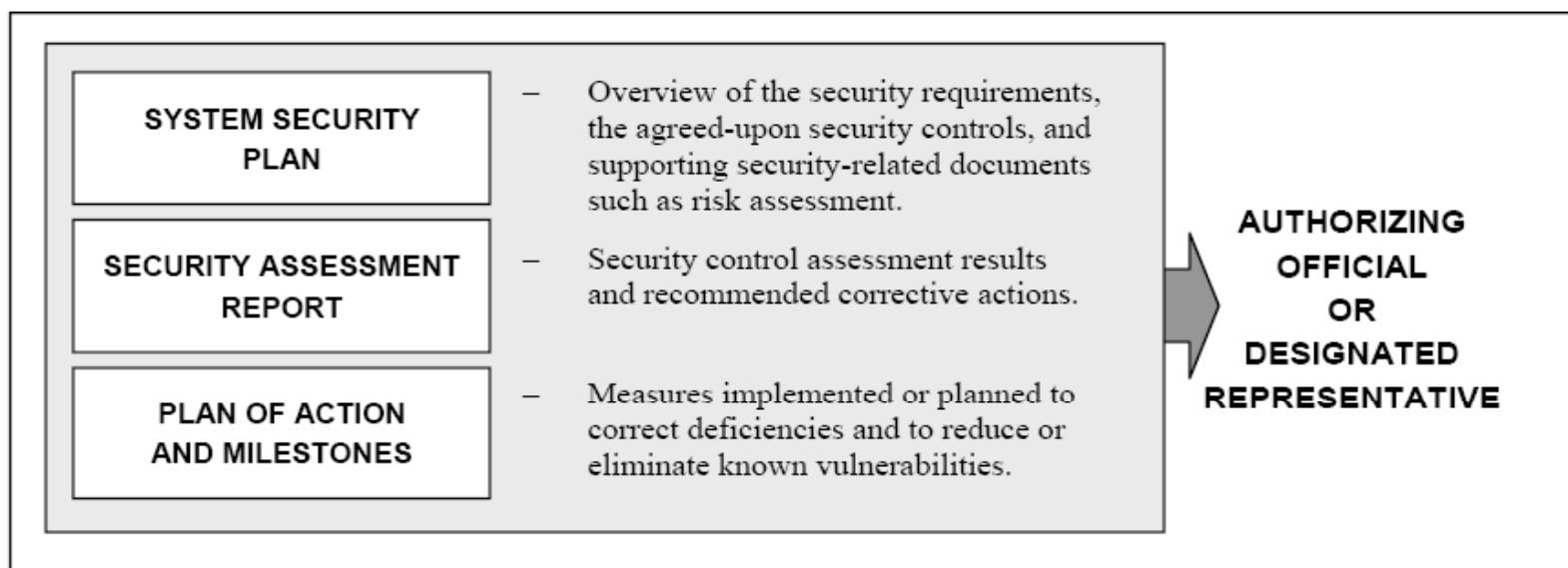
FIGURE 6-3 Special Publications Supporting SP 800-37



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

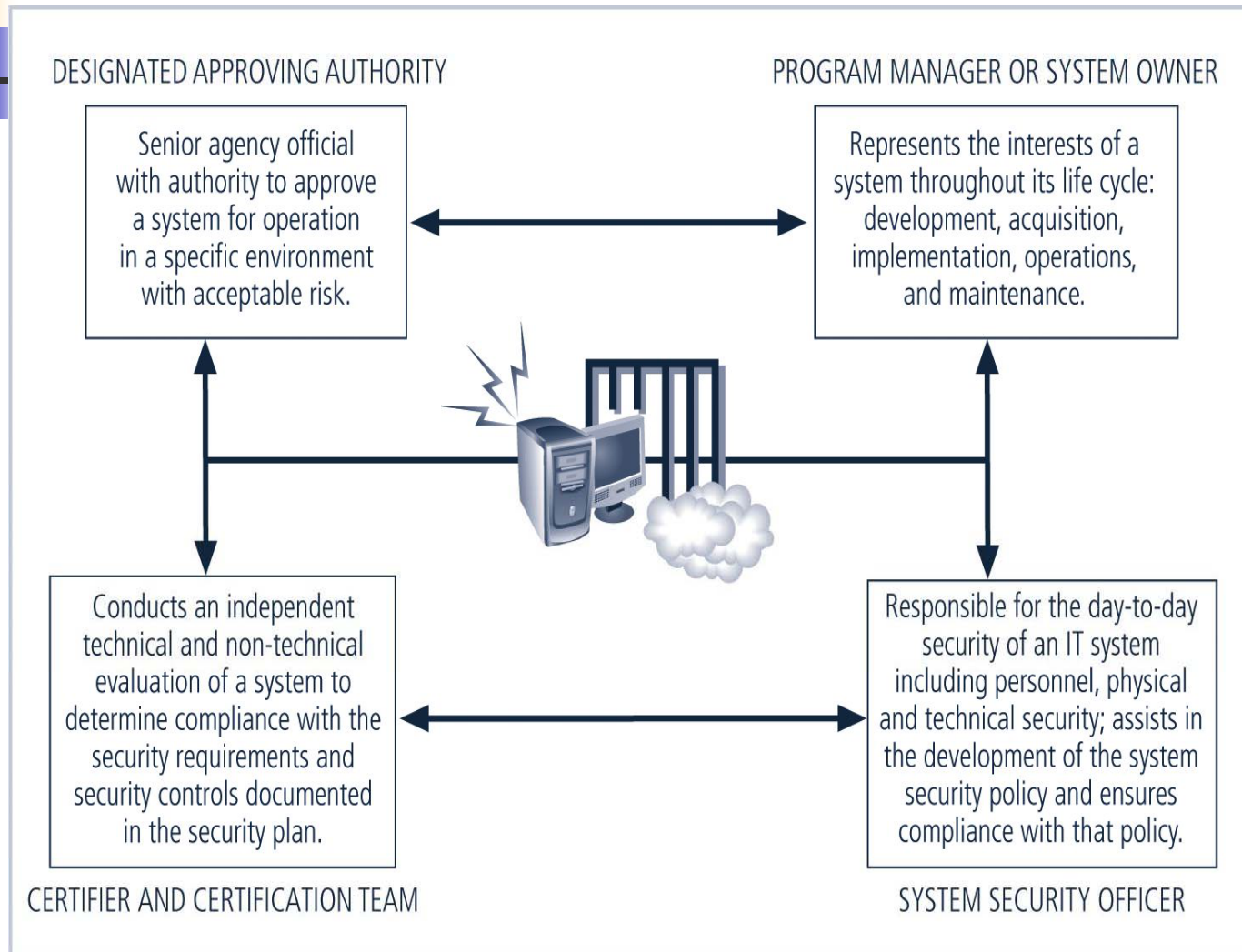
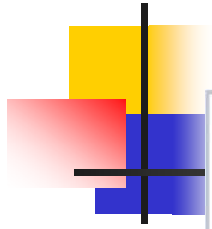


FIGURE 6-4 Participants in the Certification and Accreditation Process

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

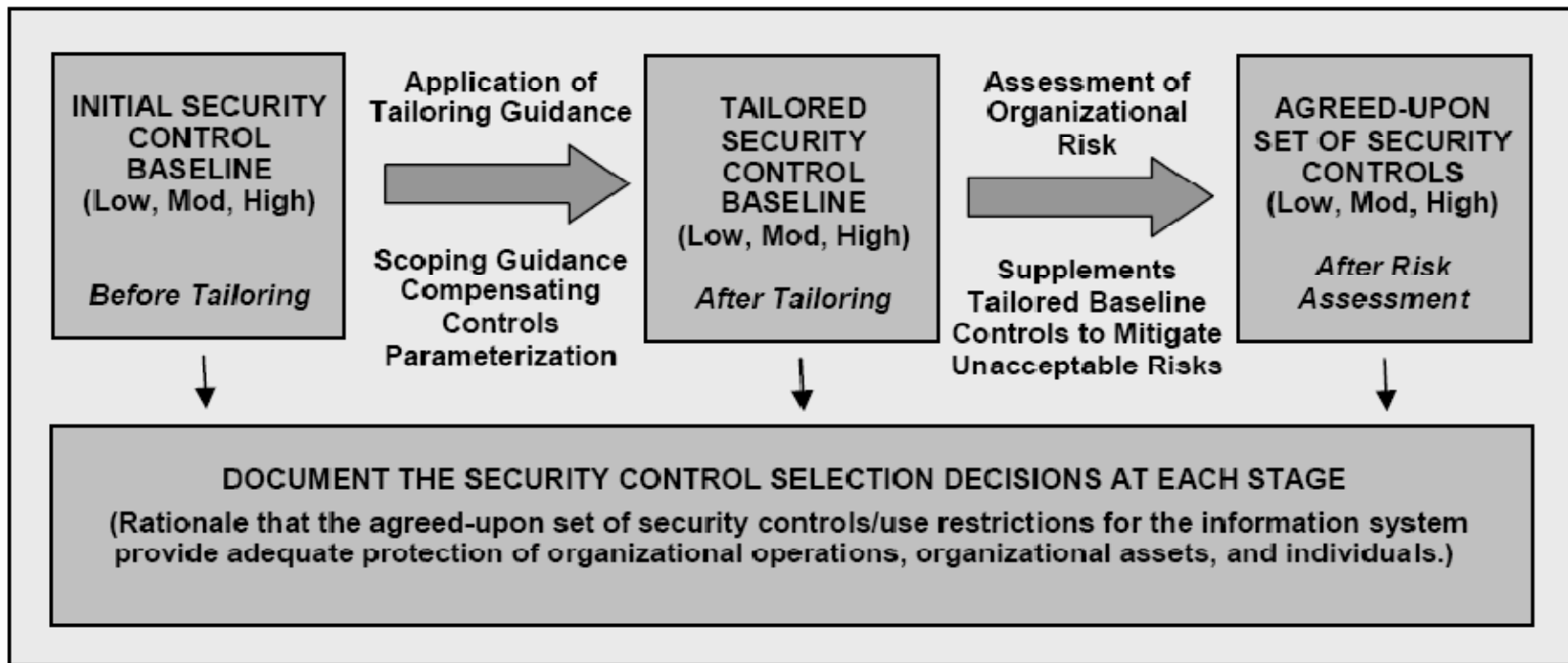


TABLE 1: SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

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)