

Roadmap

- **Developing the Security Program**

- Organizing for Security
- Placing InfoSec within an Organization
- Components of the Security Program
- InfoSec Roles and Titles
- Implementing SETA Programs



- **Security Management Models**

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





Learning Objectives

- Describe the dominant InfoSec blueprints, frameworks, and InfoSec management models
- Explain why access control is an essential element of InfoSec management
- Recommend an InfoSec management model and explain how it can be customized to meet the needs of a particular organization
- Describe the fundamental elements of key InfoSec management practices

Introduction

- InfoSec models are standards that are used for reference or comparison and often serve as the stepping-off point for emulation and adoption
- A number of published InfoSec models and frameworks exist, including options from governments and from standards organizations
- One may need to modify or adapt portions of several frameworks; what works well for one organization may not precisely fit another.



Blueprints, Frameworks, and Security Models

- To create or maintain a secure environment
 - Design a working security plan
 - Implement a management model to execute and maintain the plan
- Begin by creating or validating a security framework followed by the development of an information security blueprint.
 - **Blueprint:** describes existing controls and identifies other necessary security controls.

Blueprints, Frameworks, and Security Models (cont'd.)

- **Framework**

- The outline of the more thorough and organization-specific blueprint, which is the basis for the design, selection, and implementation of all subsequent security controls

- Most organizations draw from established security models and practices to develop a blueprint or methodology

- A **security model** is a generic blueprint offered by a service organization.

Access Control Models

- **Access controls**

- Regulate the admission of users into trusted areas of the organization
 - ✓ Both the logical access to the information systems and the physical access to the organization's facilities
- Maintained by means of a collection of policies, programs to carry out those policies, and technologies that enforce policies
- Applications: identification, authentication, authorization and accountability

Three key principles of access control

- **Least privilege:** The principle by which members of the organization can access the minimum amount of information for the minimum amount of time necessary to perform their required duties
- **Need to Know:** This principle limits a user's access to the specific information required to perform the currently assigned task, and not merely to the category of data required for a general work function
- **Separation of Duties:** This principle requires that significant tasks be split up in such a way that more than one individual is responsible for their completion

Categories of Access Control

A number of approaches are used to categorize access control methodologies. One approach depicts controls by their inherent characteristics

- **Preventative:** helps an organization avoid an incident
- **Deterrent:** discourages or deters an incipient incident
- **Detective:** detects or identifies an incident or threat when it occurs
- **Corrective:** remedies a circumstance or mitigates damage done during an incident
- **Recovery:** restores operating conditions back to normal
- **Compensating:** resolves shortcomings

Categories of Access Control (cont'd.)

A second approach, by NIST SP Series: categories controls based on operational impact to the organization

- **Management:** Controls that cover security processes that are designed by strategic planners and routinely used to design, implement, and monitor other control systems
- **Operational:** Controls that deal with the operational functions of security that have been integrated into the repeatable processes of the organization
- **Technical:** Controls that support the tactical portion of a security program and deal with the immediate needs of the organisation.

Categories of Access Control (cont'd.)

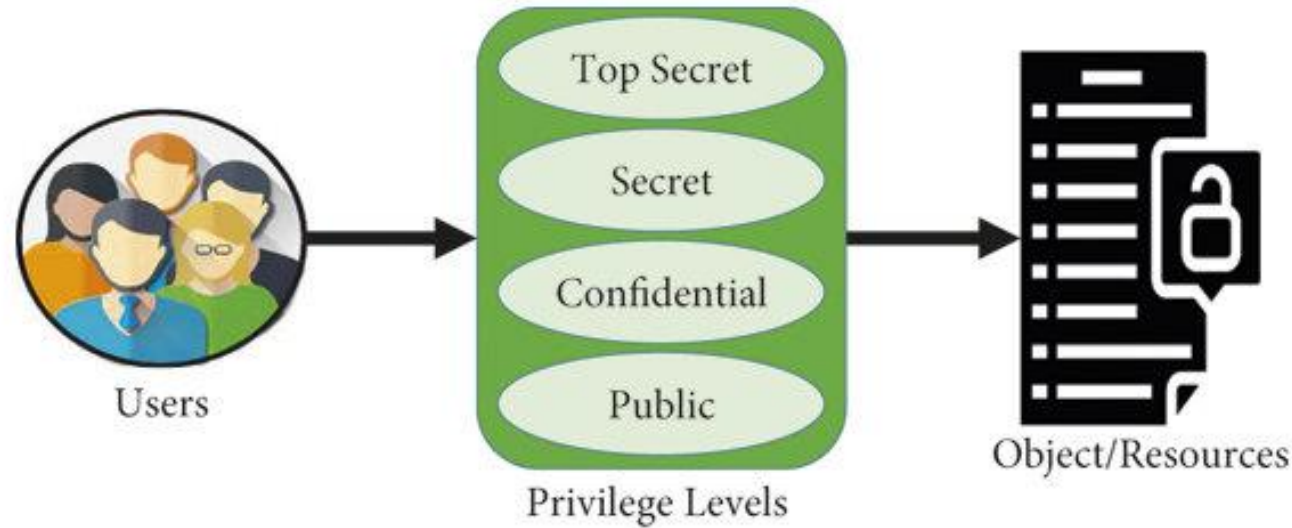
	Deterrent	Preventative	Detective	Corrective	Recovery	Compensating
Management	Policies	Registration procedures	Periodic violation report reviews	Employee or account termination	Disaster recovery plan	Separation of duties, job rotation
Operational	Warning signs	Gates, fences, and guards	Sentries, CCTVs	Fire suppression systems	Disaster recovery procedures	Defense in depth
Technical	Warning banners	Login systems, Kerberos	Log monitors and IDPSs	Forensics procedures	Data backups	Key logging and keystroke monitoring

Source: © NIST SP 800 Series.

Categories of Access Control (cont'd.)

The third approach describes the degree of authority under which the controls are applied:

- **Mandatory Access Controls (MACs)**
- **Nondiscretionary Controls**
- **Discretionary Access Controls (DACs)**



• **Mandatory Access Controls (MACs)**

- Structured and coordinated within a data classification scheme that rates each collection of information as well as each user
- These ratings are often referred to as sensitivity levels
- When MACs are implemented, users and data owners have limited control over access to information resources

Data Classification Model

The U.S. military classification scheme relies on a more complex five-level classification scheme (as defined in Executive Order 12958):

- Unclassified data - Generally free for distribution to the public
- Sensitive but unclassified (SBU) data
- Confidential data - cause damage to the national security
- Secret data - cause serious damage to the national security
- Top secret data - cause exceptionally grave damage to the national security



Data Classification Model (cont'd)

- Most organizations do not need the detailed level of classification used by military or federal agencies
- Data owners must classify the information assets for which they are responsible and review the classifications periodically
- Example of classification types:
 - Public—For general public dissemination,
 - For official use only—Not for public release but not particularly sensitive
 - Sensitive—Important information
 - Classified—Essential and confidential information



- **Personnel security clearance structure**

- Each user of an information asset is assigned an authorization level
 - ✓ Indicates the level of information classification they may access
- Most organizations have developed roles and corresponding security clearances
 - ✓ Individuals are assigned into groups that correlate with the classifications of the of information assets they need for their work

• Security clearances (cont'd)

➤ In the need-to-know principle, regardless of one's security clearance, an individual is not allowed to view data simply because it falls within that individual's level of clearance

✓ Must have a business-related need to know

✓ Hence ensures the confidentiality of information





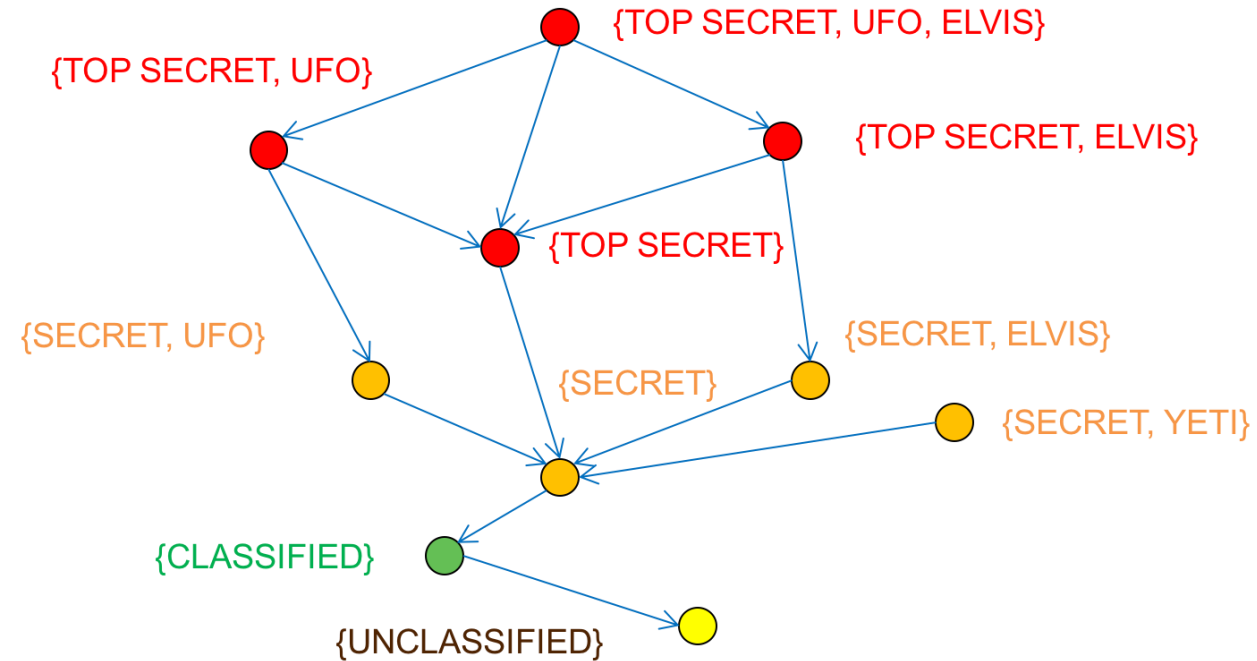
• Managing an information asset

- Considering its storage, distribution, portability, and destruction
- An information asset that has a classification designation other than unclassified or public must be clearly marked as such
 - ✓ Must be available only to authorized individuals
- To maintain the confidentiality of classified documents, managers can implement a clean desk policy
- When copies of classified information are no longer valuable or too many copies exist, care should be taken to destroy them properly to discourage dumpster diving



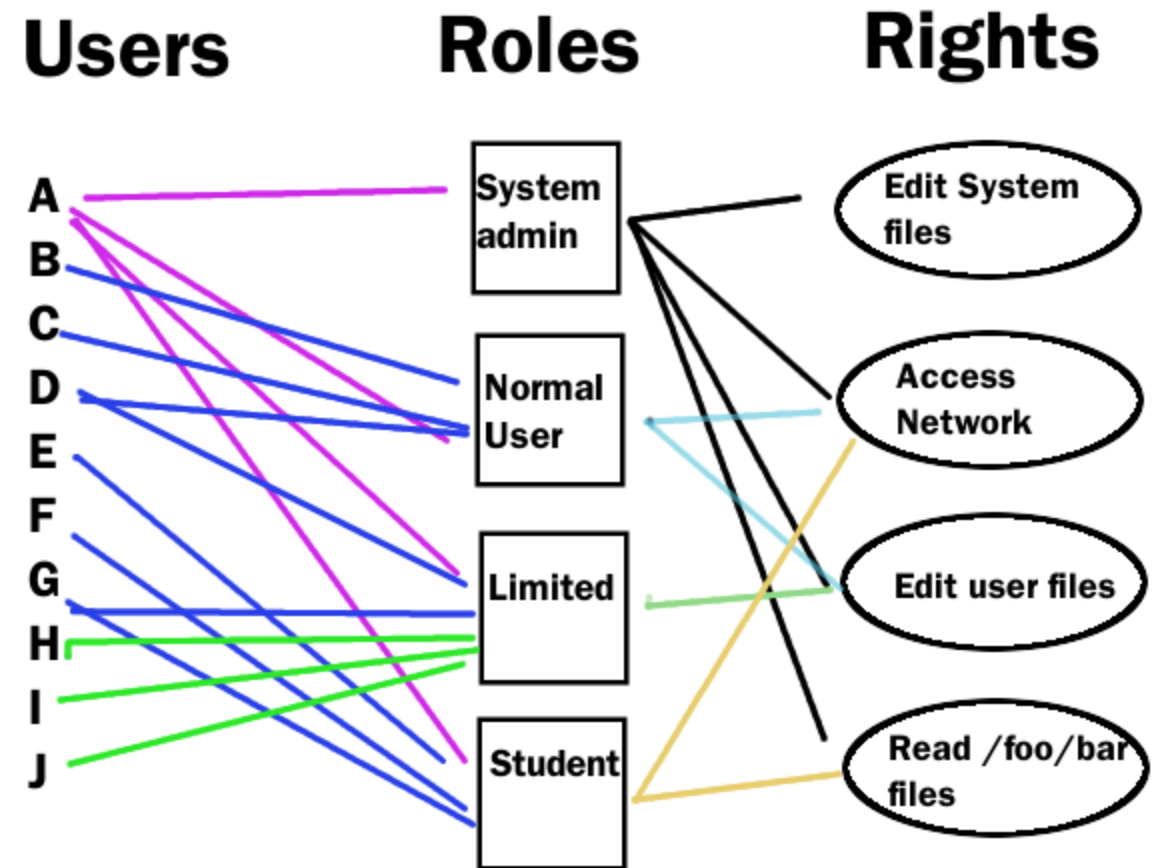
• Lattice-Based Access Control

- A variation on the MAC form of access control
- Assigns users a matrix of authorisations for particular areas of access
- The level of authorisation can vary
 - ✓ Depending on individual's classification authorisation for each group of information assets
- Lattice structure contains subjects and objects, and the boundaries associated with each subject/object pair are clearly demarcated

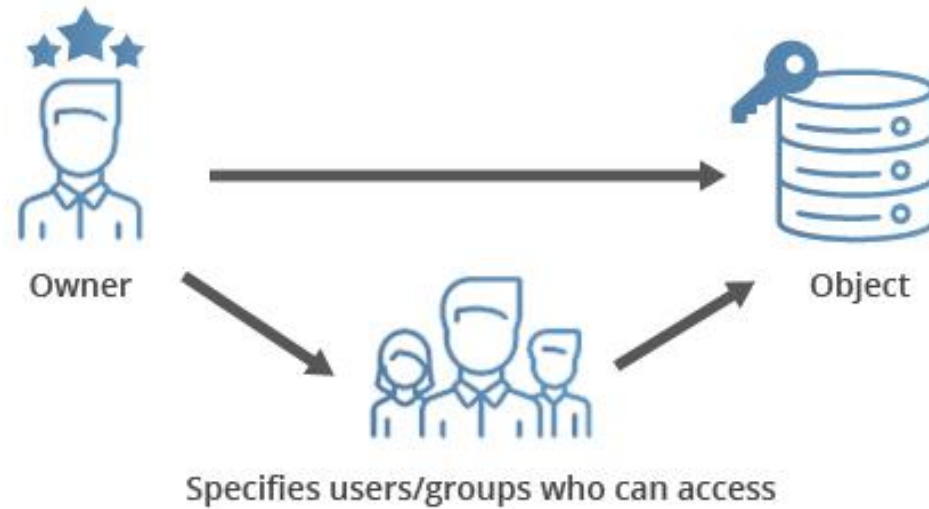


• **Nondiscretionary access controls**

- Determined by a central authority in the organization
- Can be role-based or task-based
- Role-based controls (RBAC) are tied to a particular user's role in an organization
- Task-based controls are tied to a particular assignment or responsibility



Discretionary Access Control (DAC)



- **Discretionary Access Controls (DACs)**

- Implemented at the option of the data user
- Users can allow general, unrestricted access, or they can allow specific individuals or sets of individuals to access the resources
- Most personal computer operating systems are designed based on the DAC model
- One discretionary model is rule-based access controls where access is granted based on a set of rules specified by the central authority

Categories of Access Control (cont'd.)

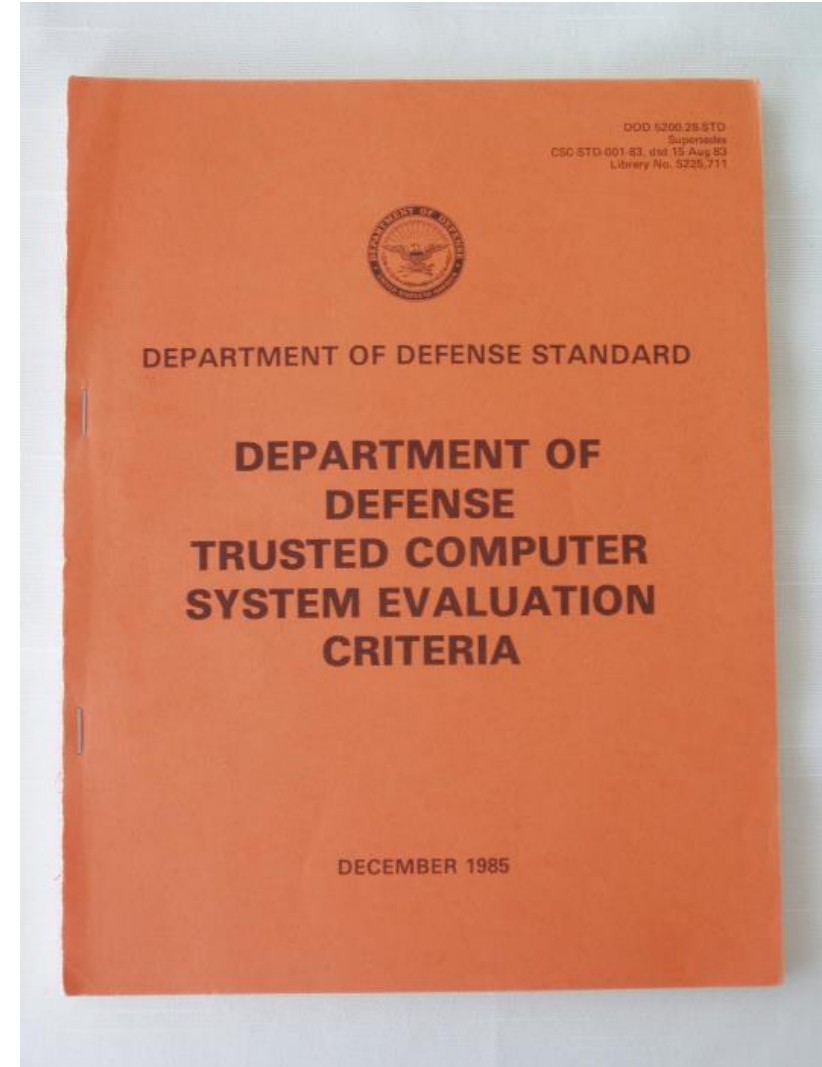
- **Other forms of access control**
 - Content-dependent access control
 - Constrained user interfaces
 - Temporal (time-based) isolation

Security Architecture Models

- Illustrate InfoSec implementations
- Can help organisations quickly make improvements through adaptation
 - Some models are implemented into computer hardware and software
 - Some are policies and practices
 - Some are implemented in both
 - Some models focus on the confidentiality of information, while others focus on the integrity of the information as it is being processed
- Trusted Computing Base, Information Technology System Evaluation Criteria, The Common Criteria: used as evaluation models.
- Bell-LaPadula, Biba: used as demonstrations of models implemented in some computer security systems

Trusted Computing Base

- **Trusted Computer System Evaluation Criteria (TCSEC)**
 - U.S. Government Department of Defense standard that defines criteria for assessing access controls in a computer system
 - Part of a larger series of standards collectively referred to as the Rainbow Series, due to the color-coding used to uniquely identify each document
 - ✓ Also known as the "Orange Book" and is considered the cornerstone of the series



Trusted Computing Base (cont'd)

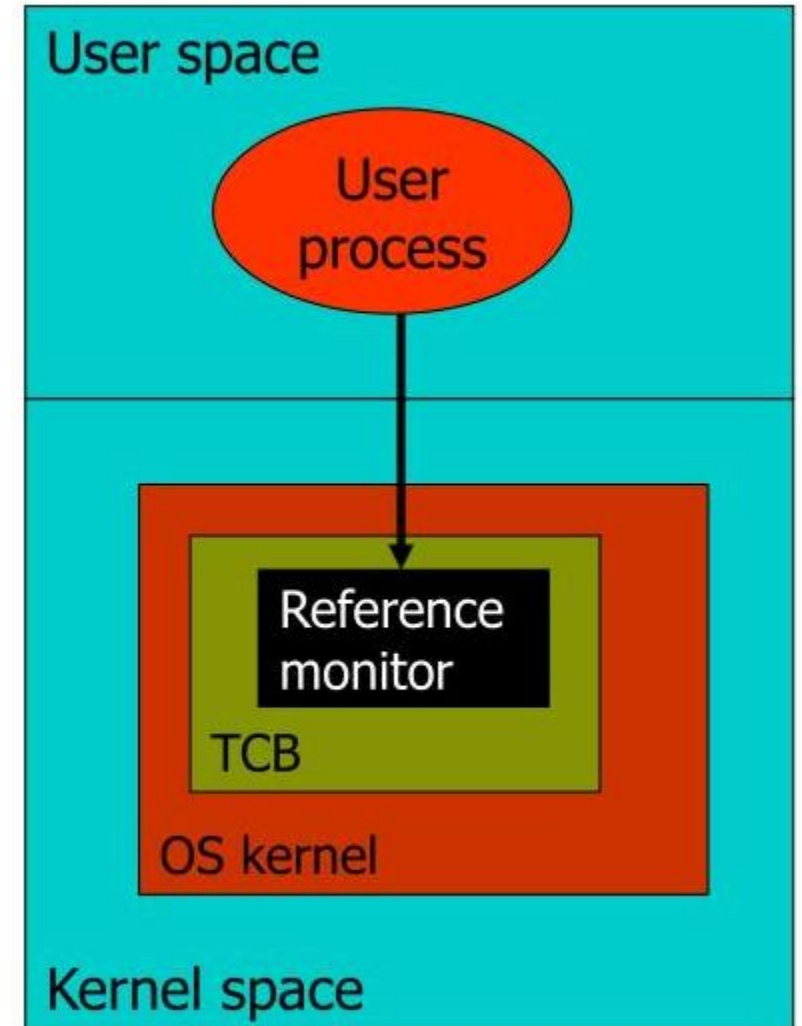
- **Trusted Computing Base (TCB)**

- The combination of all hardware, firmware, and software responsible for enforcing the security policy (MAC for VPN access)
 - ✓ In this context, security policy refers to the rules of configuration for a system, rather than a managerial guidance document
- Made up of the hardware and software that has been implemented to provide security for a particular information system

Trusted Computing Base (cont'd)

- **Reference monitor**

- A conceptual object
- The piece of the system that manages access controls, i.e., it mediates all access to objects by subjects
- Systems administrators must be able to audit or periodically review the reference monitor to ensure it is functioning effectively, without unauthorised modification



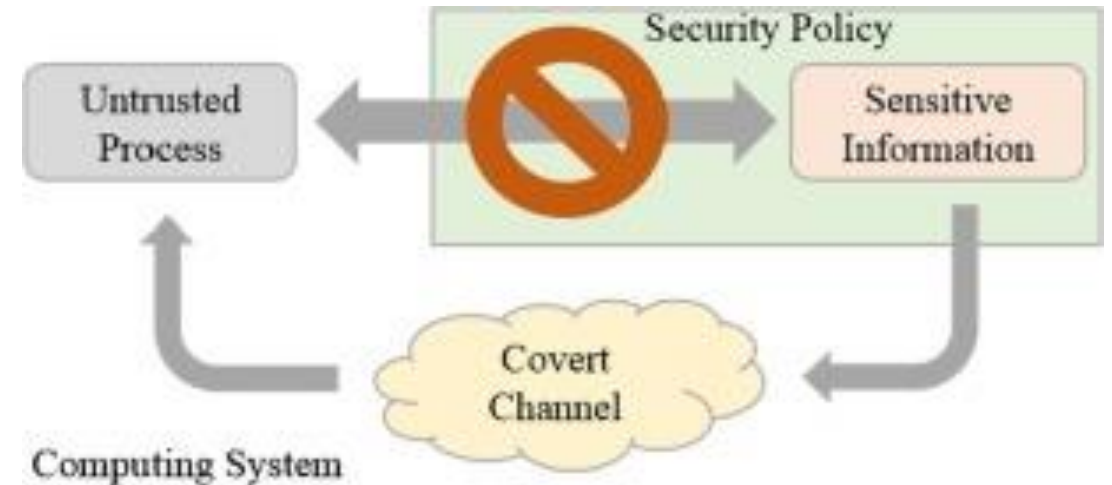
Trusted Computing Base (cont'd)

- **Covert channels**

- Unauthorised or unintended methods of communications hidden inside a computer system

- **Types of covert channels**

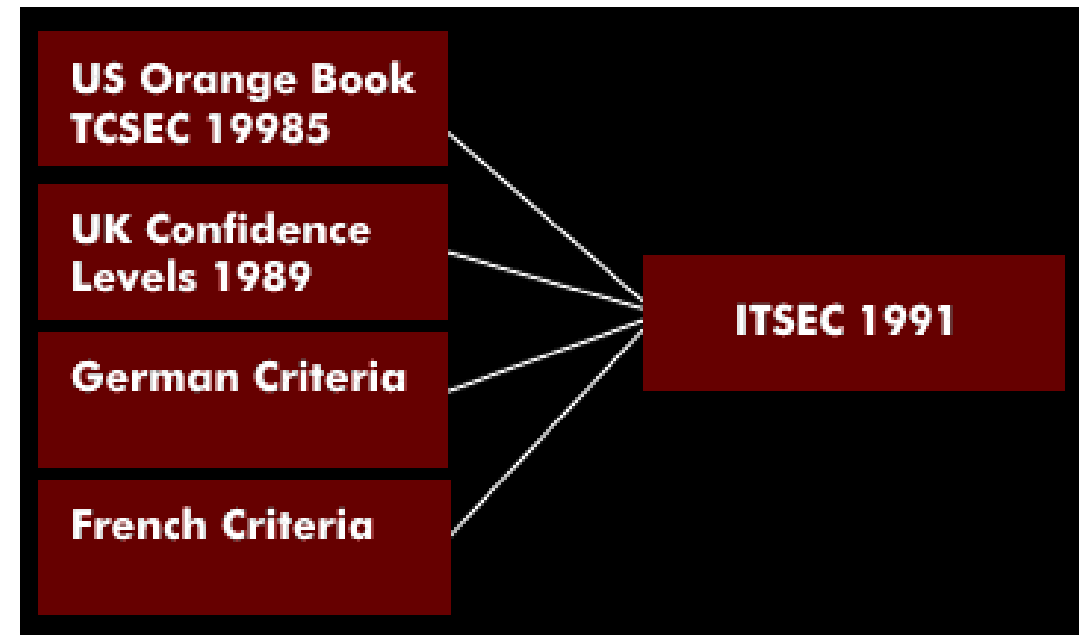
- ✓ Storage channels, which communicate by modifying a stored object
 - ✓ Timing channels, which transmit information by managing the relative timing of events



Information Technology System Evaluation Criteria

- **Information Technology System Evaluation Criteria (ITSEC)**

- An international set of criteria for evaluating computer systems, is very similar to TCSEC.
- Under ITSEC, Targets of Evaluation (ToE) are compared to detailed security function specifications, resulting in an assessment of systems functionality and comprehensive penetration testing.
- Replaced by the Common Criteria

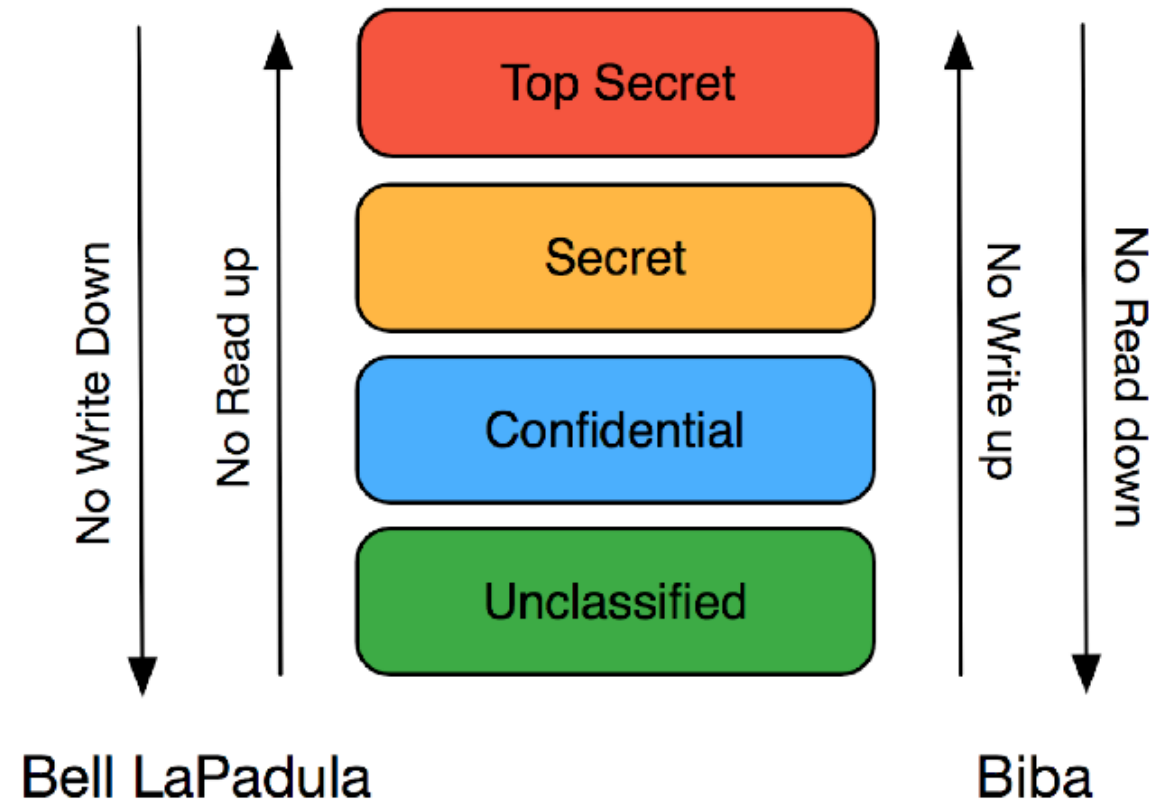




- **Common Criteria for Information Technology Security Evaluation (often called “Common Criteria” or “CC”)**
 - An international standard (ISO/IEC 15408) for computer security certification
 - Considered the the successor to both TCSEC and ITSEC
 - Combined effort of contributors from many countries (Australia, New Zealand, Canada, France, Germany, Japan, the Netherlands, Spain, the United Kingdom, and the United States)

The Bell-LaPadula Confidentiality Model & the BiBa Integrity Model

- **The Bell-LaPadula (BLP) confidentiality model:**
prevents information from being moved from a level of higher security to a level of lower security
- **The BiBa integrity model:**
ensures that no information from a subject can be passed on to an object in a higher security level



Other Models

- **The Clark-Wilson integrity model**

- Built upon principles of change control rather than integrity levels; designed for the commercial environment
- Establishes a system of subject-program-object relationships such that the subject has no direct access to the object.

- **The Brewer-Nash Model (Chinese Wall)**

- Designed to prevent a conflict of interest between two parties.
- Requires users to select one of two conflicting sets of data, after which they cannot access the conflicting data

- **Graham-Denning Access Control Model, Harrison-Ruzzo-Ullman Model**

Security Management Models: The ISO 27000 Series

- **Information Technology – Code of Practice for Information Security Management**
 - One of the most widely referenced and discussed security models
 - Originally published as British Standard 7799 and, later as ISO/IEC 17799
 - Renamed as ISO/IEC 27002 (in 2007)
 - ISO/IEC 27001 provides information on how to implement ISO/IEC 27002 and how to set up an information security management system (ISMS).
- Establishes guidelines for initiating, implementing, maintaining, and improving information security management

ISO/IEC 27001

Information security management systems

Requirements

Current edition: **ISO/IEC 27001:2022**

Status: **Published** (stage 60.60)

Buy this standard

Format	Language
✓ PDF + ePub	English ▾
PDF + ePub + Redline	English ▾
Paper	English ▾

CHF 124

 Buy

What is ISO/IEC 27001?

ISO/IEC 27001 is the world's best-known standard for **information security management systems (ISMS)**. It defines requirements an ISMS must meet.

The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.

Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.

ISO/IEC 27002:2022

Information security, cybersecurity and privacy protection — Information security controls

Abstract

 **Preview**

This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

- a) within the context of an information security management system (ISMS) based on ISO/IEC27001;
- b) for implementing information security controls based on internationally recognized best practices;
- c) for developing organization-specific information security management guidelines.

General information


Status :  Published

Publication date : 2022-02
Corrected version (en) : 2022-03


Edition : 3

Number of pages : 152

Buy this standard

Format	Language
 PDF + ePub	English
PDF + ePub + Redline	English
Paper	English

CHF 208

 **Buy**

Security Management Models: NIST Security Models

- **Notable advantages of NIST documents:**

- Publicly and freely available: <https://csrc.nist.gov/publications/PubsSPs.html>
- Have been available for some time and thus have been broadly reviewed by government and industry professionals

- **NIST SP (Special Publication) 800 Series, Computer Security (December 1990-present):** NIST's primary mode of publishing computer/cyber/information security guidelines, recommendations and reference materials

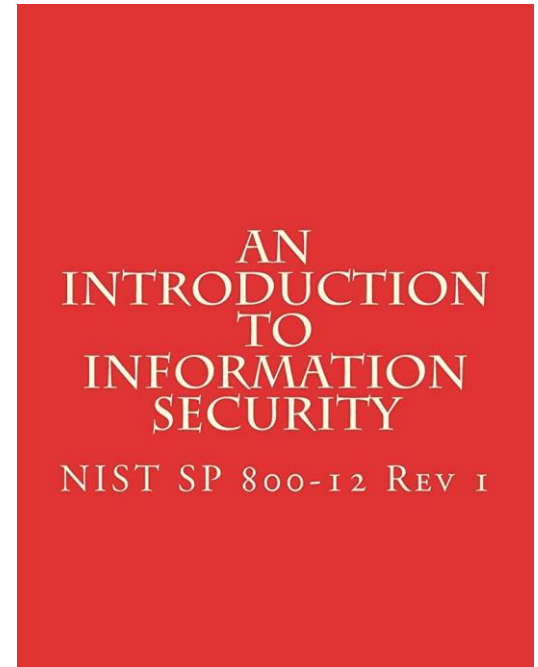
NIST SP 800 documents relevant to InfoSec managements:

- **SP 800-12 Rev. 1:** *An Introduction to Information Security (2017)*
- **SP 800-14:** *Generally Accepted Security Principles and Practices for Security Information Technology Systems (1996)*
- **SP 800-18 Rev. 1:** *Guide for Developing Security Plans for Federal Information Systems (2006)*
- **SP 800-30 Rev. 1:** *Guide for Conducting Risk Assessments (2012)*
- **SP 800-34 Rev. 1:** *Contingency Planning Guide for Federal Information Systems (2010)*
- **SP 800-37 Rev.1:** *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (2010)*
- **SP 800-39:** *Managing Information Security Risk: Organization, Mission, and Information System View (2011)*
- **SP 800-53 Rev. 4:** *Security and Privacy Controls for Federal Information Systems and Organizations (2013)*
- **SP 800-53A Rev. 4:** *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans (2014)*
- **SP 800-55 Rev. 1:** *Performance Measurement Guide for Information Security (2008)*
- **SP 800-61 Rev. 2:** *Computer Security Incident Handling Guide (2012)*
- **SP 800-100:** *Information Security Handbook: A guide for Managers (2017)*
- **SP 800-184:** *Guide for Cybersecurity Event Recovery (2016)*

- **NIST SP 800-12 Rev. 1: *An Introduction to Information Security (2017)***
 - Excellent reference and guide for the routine management of InfoSec
 - Help gain a deeper understanding of background and terminology in InfoSec

- **Content:**

1. Introduction to the SP
2. Elements of InfoSec
3. Key roles and responsibilities for both industry and government sectors
4. An overview of threat and vulnerabilities
5. Information Security Policy
6. Information Security Risk Management
7. Assurance
8. Security considerations in systems support and operations
9. Cryptography
10. Control families

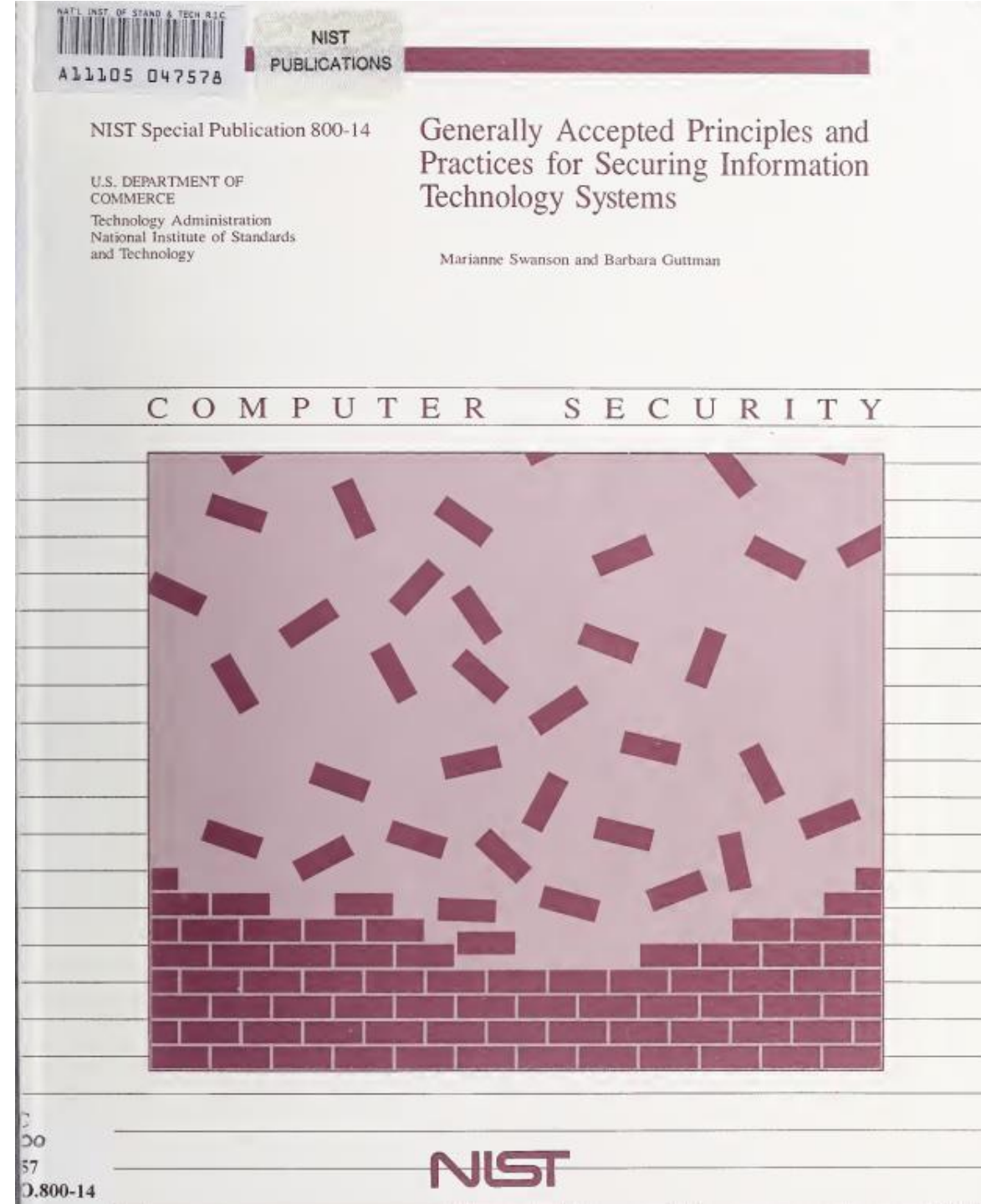


NIST SP 800-12 Rev. 1 lists 20 control families that form the foundation of the NIST security model

Access Control	Media Protection
Awareness and Training	Privacy Authorization
Audit and Accountability	Physical and Environmental Protection
Assessment, Authorization, and Monitoring	Planning
Configuration Management	Program Management
Contingency Planning	Personnel Security
Identification and Authentication	Risk Assessment
Individual Participation	System and Services Acquisition
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

NIST Special Publication 800-14:

- 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 SP 800-14: 8 Key Points

1. Security supports organization's mission
2. Security is integral to sound management
3. Security should be cost-effective
4. Systems owners have security responsibilities outside their own organizations
5. Security responsibilities and accountability should be made explicit
6. Security requires a comprehensive and integrated approach
7. Security should be periodically reassessed
8. Security is constrained by societal factors

NIST SP 800-14: 33 Principles

Principle 1	Establish a sound security policy as the “foundation” for the design
Principle 2	Treat security as an integral part of the overall system design
Principle 3	Clearly delineate the physical and logical security boundaries governed by associated security policies
Principle 4	Reduce risk to an acceptable level
Principle 5	Assume that external systems are insecure
Principle 6	Identify potential trade-offs between reducing risk and increased costs and decreases in other aspects of operational effectiveness
Principle 7	Implement layered security (ensure no single point of vulnerability)
Principle 8	Implement tailored system security measures to meet organizational security goals
Principle 9	Strive for simplicity
Principle 10	Design and operate an IT system to limit vulnerability and to be resilient in response
Principle 11	Minimize the system elements to be trusted
Principle 12	Implement security through a combination of measures distributed physically and logically

Principle 13	Provide assurance that the system is, and continues to be, resilient in the face of expected threats
Principle 14	Limit or contain vulnerabilities
Principle 15	Formulate security measures to address multiple overlapping information domains
Principle 16	Isolate public access systems from mission-critical resources (e.g., data, processes)
Principle 17	Use boundary mechanisms to separate computing systems and network infrastructures
Principle 18	Where possible, base security on open standards for portability and interoperability
Principle 19	Use a common language in developing security requirements
Principle 20	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations
Principle 21	Design security to allow for regular adoption of new technologies, including a secure and logical technology upgrade process
Principle 22	Authenticate users and processes to ensure appropriate access control decisions both within and across domains
Principle 23	Use unique identities to ensure accountability
Principle 24	Implement least privilege (process of granting the lowest level of access consistent with accomplishing the assigned role)
Principle 25	Do not implement unnecessary security mechanisms
Principle 26	Protect information while being processed, in transit, and in storage
Principle 27	Strive for operational ease of use
Principle 28	Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability
Principle 29	Consider custom products to achieve adequate security
Principle 30	Ensure proper security in the shutdown or disposal of a system
Principle 31	Protect against all likely classes of "attacks"
Principle 32	Identify and prevent common errors and vulnerabilities
Principle 33	Ensure that developers are trained in how to develop secure software

NIST Security Models (cont'd.)

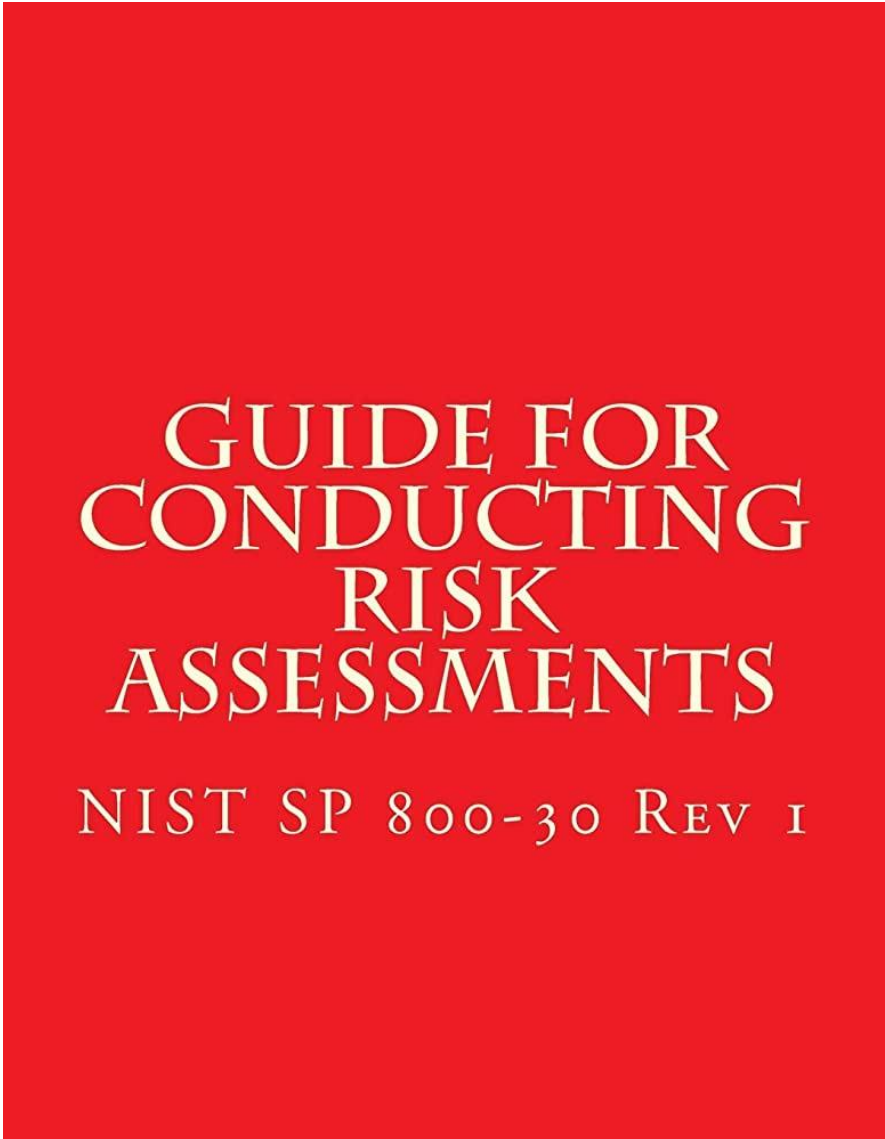
- **NIST Special Publication 800-18, Rev. 1:** *Guide for Developing Security Plans for Federal Information Systems*
 - Provides detailed methods for assessing, designing, and implementing controls and plans for various sized applications
 - Serves as a guide for the activities described in this chapter, and for the overall information security planning process
 - Includes templates for major application security plans

GUIDE FOR
DEVELOPING
SECURITY PLANS
FOR FEDERAL
INFORMATION
SYSTEMS
NIST SP 800-18 R 1

NIST Security Models (cont'd.)

- **NIST Special Publication 800-30, Rev. 1:**
Guide for Conducting Risk Assessments

- Provides a foundation for the development of an effective risk management program
- Contains 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

The image shows the front cover of the NIST Special Publication 800-30, Revision 1. The cover has a solid red background. The title 'GUIDE FOR CONDUCTING RISK ASSESSMENTS' is printed in a large, white, serif font, centered on the upper half of the cover. Below the title, the text 'NIST SP 800-30 REV 1' is printed in a smaller, white, serif font, also centered.

GUIDE FOR CONDUCTING RISK ASSESSMENTS

NIST SP 800-30 REV 1



Control Objectives for Information and Related Technology (COBIT)

- Provides advice about the implementation of sound controls and control objectives for InfoSec
- Created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992
- COBIT 5 was released in 2012.



- COBIT presents 34 high-level objectives that cover 215 control objectives
- COBIT 5: Five principles and seven enablers.
- **Five principles:**
 - Principle 1: Meeting Stakeholder Needs
 - Principle 2: Covering the Enterprise End-to- End
 - Principle 3: Applying a Single, Integrated Framework
 - Principle 4: Enabling a Holistic Approach
 - Principle 5: Separating Governance From Management



- **Seven 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



- Another control-based model is that of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission
 - Major objective: identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence.
- The COSO framework is built on 5 interrelated components
 - Control environment
 - Risk assessment
 - Control activities
 - Information and communication
 - Monitoring

Recap

- A framework is the outline of a more thorough blueprint, used in the creation of the InfoSec environment. A security model is a generic blueprint offered by a service organization.
- Access controls regulate the admission of users into trusted areas of the organization. Access control is built on the principles of least privilege, need-to-know, and separation of duties.
- Approaches to access control include preventative, deterrent, detective, corrective, recovery, and compensating. Access controls may be classified as management, operational (or administrative), or technical.
- Mandatory access controls (MACs) are those controls required by the system that operate within a data classification and personnel clearance scheme.
- Nondiscretionary controls are determined by a central authority in the organization and can be based on roles or on a specified set of tasks. Discretionary access controls (DACs) are implemented at the discretion or option of the data user.

Recap (cont'd)

- Security architecture models illustrate InfoSec implementations and can help organizations make quick improvements through adaptation. The most common models are the Trusted Computer System Evaluation Criteria (TCSEC) that includes the Bell-LaPadula (BLP) confidentiality model and the Biba integrity model.
- One of the most widely referenced security models is given by ISO 27001, which is designed to give recommendations for InfoSec management. Other approaches to structuring InfoSec management are found in many documents in the NIST SP 800 series.
- “Control Objectives for Information and Related Technology” (COBIT) provides advice about the implementation of sound controls and control objectives for InfoSec.
- The Committee of Sponsoring Organizations (COSO) of the Treadway Commission has established a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems.