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

Computer Science and Engineering

Disclaimer:

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

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

Syllabus

Unit: I	Basics of Security, Principles of Information Security Management, Need for Security: Threats, Attacks. Planning for Security, The role of Planning, Information Security Governance. Information Security Policy, Standards, and Practices, Planning for Information Security Implementation, Types of Information Security Policy, Guidelines for Effective Policy, Information Security Roles and Titles. Security Education, Training, and Awareness Program.	**9 Hrs**
Unit: II	**Security Management Model** Blueprints, Framework and Security Models, Access Control Models, Security Architecture Models, Security Management Models- ISO 270000 Series, NIST Security Models, SP 800-53A, COBIT, COSO, IT Infrastructure Library, Information Security Governance Framework.	**9 Hrs**
Unit: III	**Implementing Security Management** Information Security Project Management, Benchmarking, Performance Measure in Information Security Management-InfoSec Performance Measure: Management, Metrics, Building, Collecting, Implementing, Reporting, Emerging Trends in Certification and Accreditation - SP 800-37, SP 800-53, Security Management Practices and Auditing.	**9 Hrs**

Syllabus (Continue)

Unit: IV	**Legal Framework and Cyber Law** Introduction, Cybercrime and the Legal Landscape around the World, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Digital Signatures and the Indian IT Act, Amendments to the Indian IT Act.	**9 Hrs**
Unit: V	**Cyber law for Cybercrime** Need for Cyber Law, Cyber Jurisprudence at International and Indian Level, Cybercrime and Punishment, Cyber Crimes & Legal Framework Cyber Crimes against Individuals, Institution and State, Hacking, Digital Forgery, Case studies.	**9 Hrs**
Books:- (Text)	1. Principles of Information Security, Michael E. Whitman, Herbert J. Mattord 2. Cyber Security, understanding cybercrimes, computer forensics and legal perspectives by Nina Godbole, and Sunit Belapure, WILEY Publication (2011), ISBN: 9788126521791.	
Books:- (Reference)	1. Sennewald, C., and Baillie, C. (2011). Effective Security Management. Elsevier Publication. 2. Handbook of Information Security Management, Micki Krause, Harold F. Tipton, Isc2 Press. 3. Security Management Models, William O. Douglas, U.S. Supreme Court Justice 4. Information Security Policies, Procedures, and Standards - A Practitioner's Reference by Douglas Landoll. CRC Press, 2016 ISBN: 1482-24589-2 5. Cyber Crime Manual by Bibhas Chatterjee, Lawman Publication	

Unit 2: Security Management Model

Blueprints, Framework and Security Models, Access Control Models,

Security Architecture Models- Trusted Computing Base Model, Bell-LaPadula Confidentiality Model, Biba Integrity Model ,Clark-Wilson Integrity Model Graham-Denning Access Control Model , Harrison-Ruzzo-Ullman, Brewer-Nash Model

Security Management Models- ISO 270000 Series, NIST Security Models, COBIT, COSO, IT Infrastructure Library, Information Security Governance Framework.

Security Management Model

A **security management model** is meant to be a **generic** description of **what** an organization should do to provide a secure environment for itself. It is generic in that it describes **what** should be done, but not **how** to do it, which makes it flexible enough to be used by many kinds of organizations.

You should choose a model for your organization to follow that is "flexible, scalable, robust, and sufficiently detailed".

Once your organization chooses a **security management model**, it should create a custom version of it that applies to your organization. The text refers to this as your **security blueprint**.

In the course of developing your security blueprint, you may need to create an outline to follow, which the text calls your **security framework**.

To put those terms in perspective, imagine three phases of a project to develop your security management standards:

- First, select a security management **model** that fits your organization's needs and goals.
- Second, write a security **framework** document, a **plan** that **outlines** the work needed to **adapt the model** to the realities of your organization.
- Third, create the security **blueprint**, which is a working, **operational** document. It describes how your organization will **meet** each applicable requirement of your security model, through the goals that are established in your framework.

- The communities of interest accountable for the security of an organization's information assets must design a **working security plan** and then implement a management model to execute and maintain that plan.
- This may begin with the creation or validation of a security framework, followed by an InfoSec blueprint that describes existing controls and identifies other necessary security controls
- These documents form the basis for the design, selection, and initial and ongoing implementation of all subsequent security controls, including policy, SETA and technologies.
- To generate a usable security blueprint, most organizations draw on established security frameworks, models, and practices.
- Another way to create a blueprint is to look at the paths taken by other organizations
- In this kind of benchmarking, you follow the recommended practices or industry standards

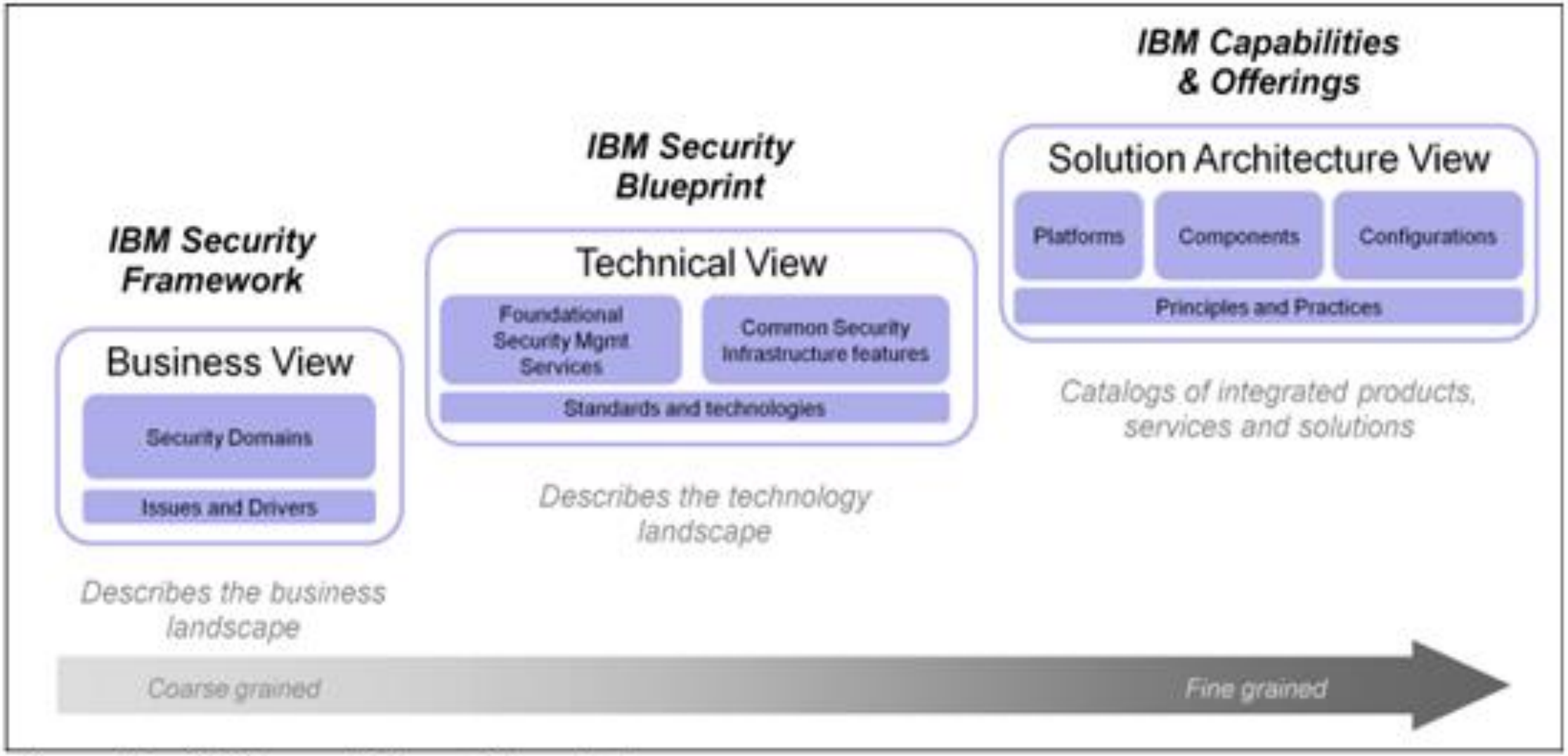


Figure 1-9 IBM Security Blueprint positioning

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

- access to systems
- access to storage
- access to physical areas
- access to communications

The general application of access control comprises four processes:

– obtaining the identity of the entity requesting access to a logical or physical area (identification)
– confirming the identity of the entity seeking access to a logical or physical area (authentication)
– determining which actions an authenticated entity can perform in that physical or logical area (authorization)
– and finally, documenting the activities of the authorized individual and systems (accountability)

Key principles of access control

1. 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
2. Need to Know
   - 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
3. Separation of Duties
   - A control requiring that significant **tasks be split up** in such a way that more than one individual is responsible for their completion

Categories of Access Control

1. Preventative – controls that help to **avoid** an incident
2. Deterrent – controls that **discourage** or deter an incident
3. Detective – controls that **detect** or identify an incident
4. Corrective – controls that remedy a circumstance or **mitigate** damage done during an incident
5. Recovery – controls that **restore** operating conditions back to normal
6. Compensating – controls that **resolve** shortcomings

NIST* Access Control categories are based on operational impact to the organization

A. Management

B. Operational (or administrative)

C. Technical

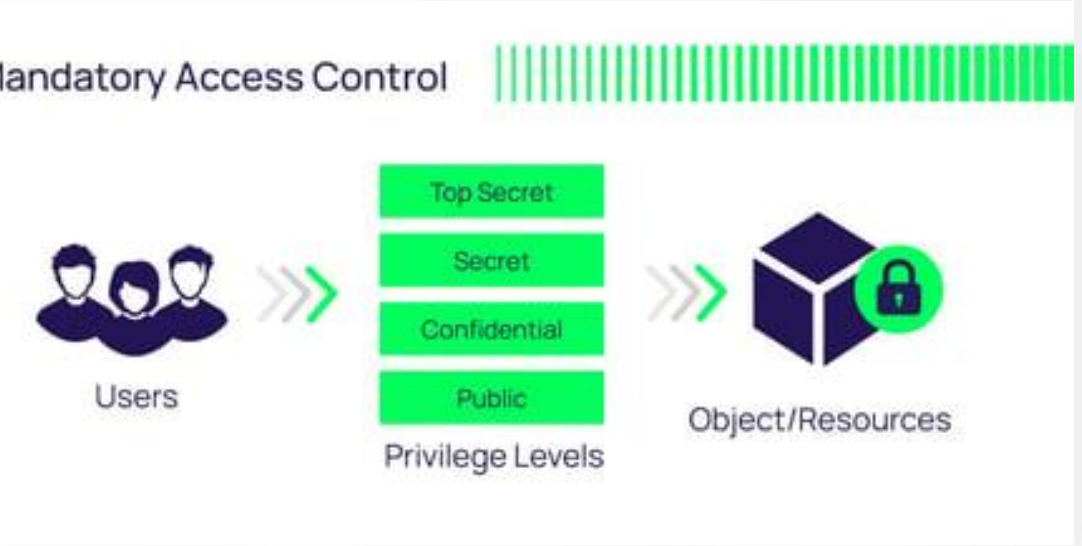
	Deterrent	Preventative	Detective	Corrective	Recovery	Compensating
Management	Policies	Registration procedures	Periodic violation report reviews	Employee or account termination	Disaster recovery plan	Separation of duties, job rotation
Operational	Warning signs	Gates, fences, and guards	Sentries, CCTVs	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

Access control models

1. Mandatory Access Control (MAC)
2. Role-Based Access Control (RBAC)
3. Discretionary Access Control (DAC)
4. Rule-Based Access Control (RBAC or RB-RBAC)

Access Control Model

- **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
  - MAC uses “security labels” to assign resource objects on a system.
  - There are two pieces of information connected to these security labels: classification (high, medium, low) and category (specific department or project – provides “need to know”).



- MAC was associated with a numbering system that would assign a level number to files and level numbers to employees. This system made it so that if a file (i.e. myfile.ppt) had is level 400, another file (i.e. yourfile.docx) is level 600 and the employee had a level of 500, the employee would not be able to access “yourfile.docx” due to the higher level (600) associated with the file.
- MAC is the highest access control and is utilized in military and/or government settings utilizing the classifications of Classified, Secret, and Unclassified in place of the numbering system previously mentioned.

Role-Based Access Control

- System administrators need to assign rights based on organizational roles instead of individual user accounts within an organization.
- It presents an opportunity for the organization to address the principle of ‘least privilege’. This gives an individual only the access needed to do their job, since access is connected to their job.

Access Control Model

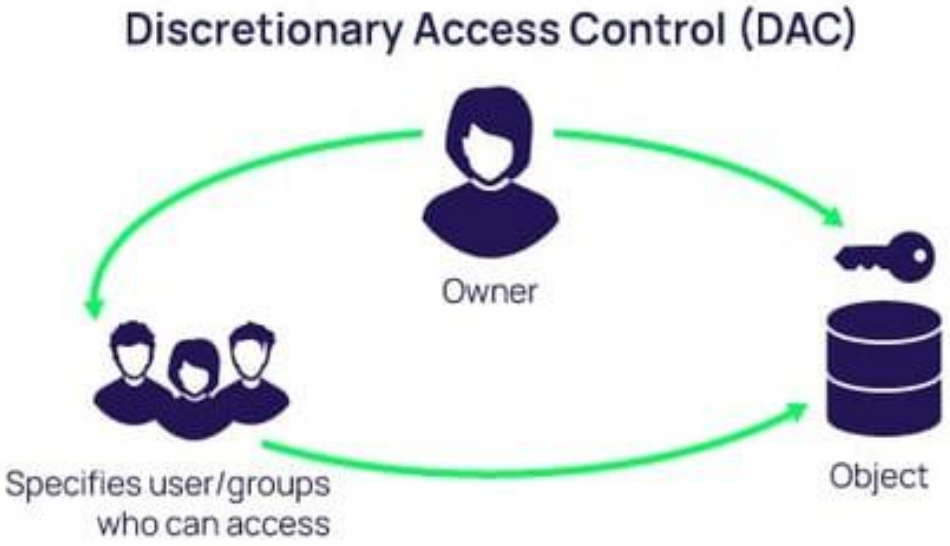
- **Discretionary Access Controls (DACs)**

  – Model is the least restrictive model compared to the most restrictive MAC model.

  – DAC allows an individual complete control over any objects they own along with the programs associated with those objects

  – Users can allow general, unrestricted access, or they can allow specific individuals or sets of individuals to access the resources.

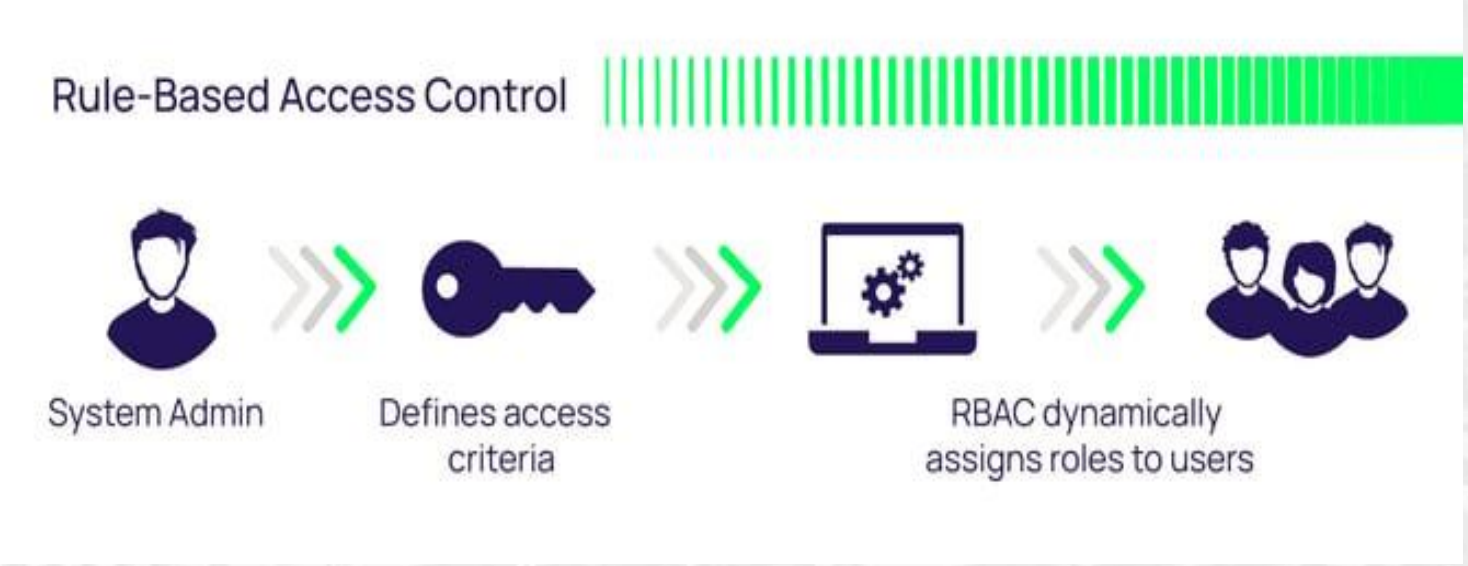
  – Most *personal computer operating systems* are designed based on the DAC model.



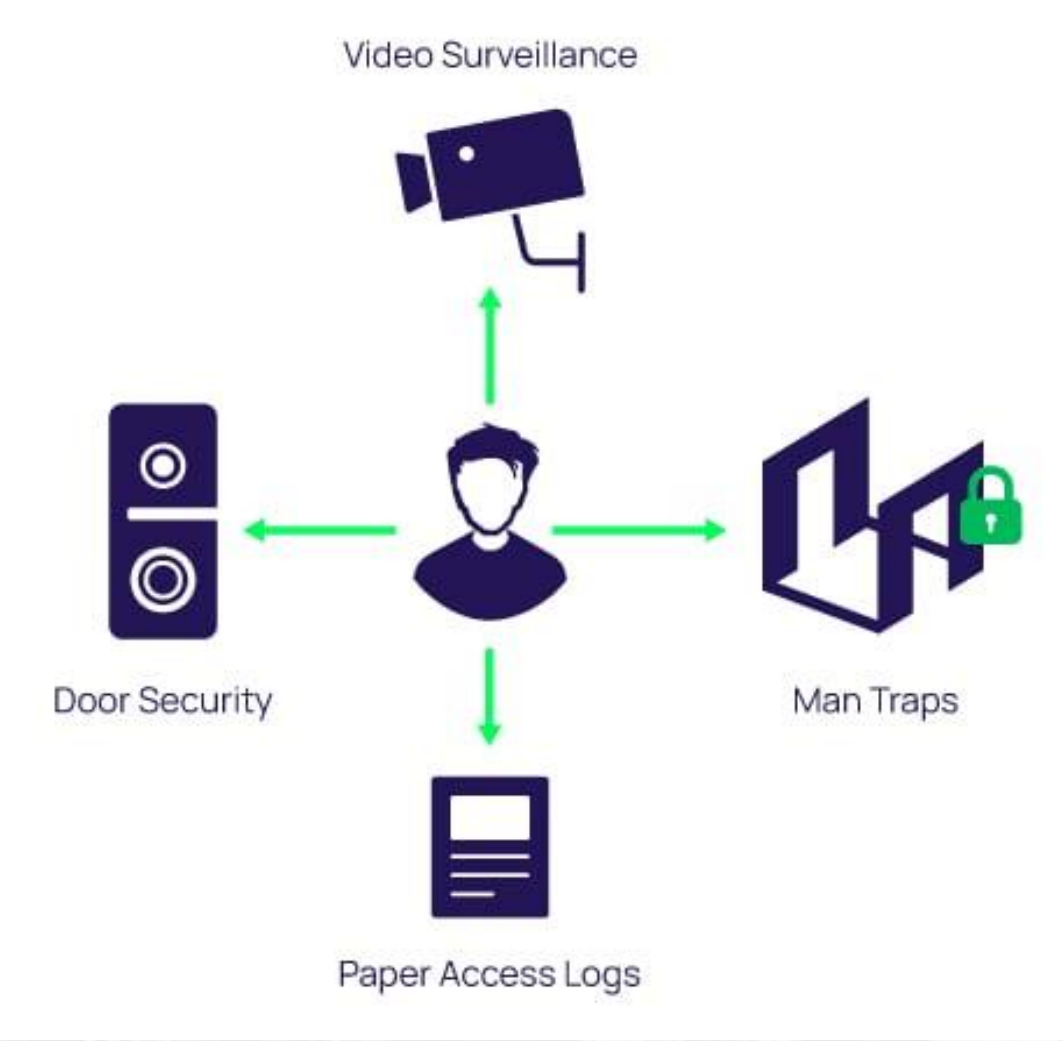
- DAC two major weaknesses:
  - First, it gives the end-user complete control to set security level settings for other users which could result in users having higher privileges than they're supposed to.
  - Secondly, and worse, the permissions that the end-user has are inherited into other programs they execute. This means the end-user can execute malware without knowing it and the malware could take advantage of the potentially high-level privileges the end-user possesses.

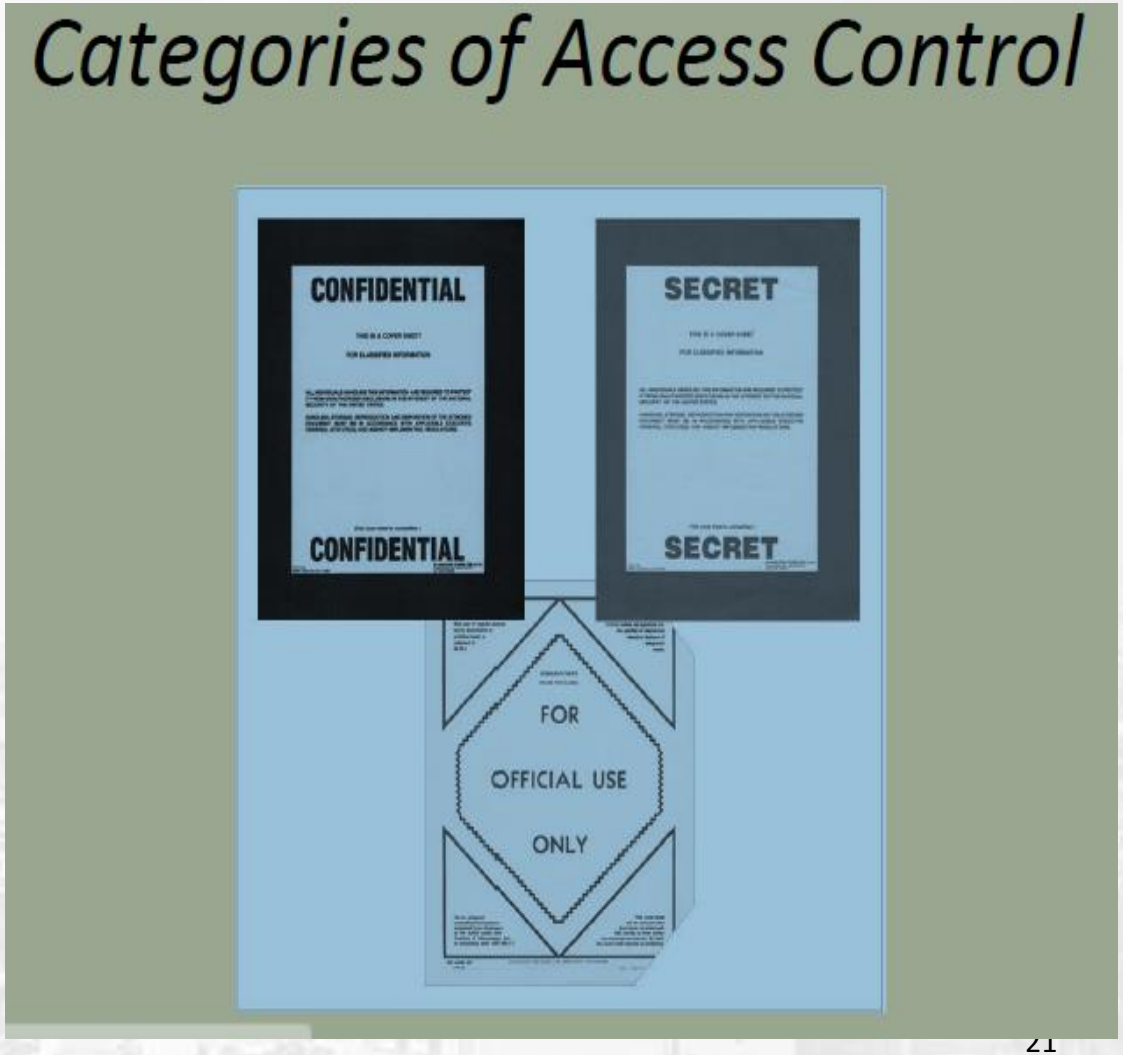
Access Control Model

- **Rule-Based Access Control**
  - Rule-Based Access Control will dynamically assign roles to users based on criteria defined by the custodian or system administrator.
  - For example, if someone is only allowed access to files during certain hours of the day, Rule-Based Access Control would be the tool of choice.



Physical Access Control





Security Architecture Models

- Illustrate InfoSec implementations
- Can help organizations 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.

Security Policy

"Subjects need to be authorized to access objects."

Security Model

- Derive the mathematical relationships and formulas explaining how *x* can access *y* only through outlined specific methods.
- Develop specifications to provide a bridge to what this means in a computing environment and how it maps to components and mechanisms that need to be coded and developed.

Example

- Write the program code to produce the mechanisms that provide a way for a system to use access control lists and give administrators some degree of control. This mechanism presents the network administrator with a GUI representation, like check boxes, to choose which subjects can access what objects, within the operating system.

Security Architecture Models

1) Trusted Computing Base Model (Authorization)
2) Bell-LaPadula Confidentiality Model (confidentiality)
3) Biba Integrity Model (integrity)
4) Clark-Wilson Integrity Model (Access Control (AC))
5) Graham-Denning Access Control Model (AC)
6) Harrison-Ruzzo-Ullman (AC)
7) Brewer-Nash (Chinese Wall) (AC – prevent conflict)

1) Trusted Computing Base Model

Trusted Computer System Evaluation Criteria (TCSEC)

– United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into 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
- 7 Evaluation Classes: D, C1, C2, B1, B2, B3, A1

– It was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information.

- A typical example in the UNIX system is the TCB includes kernel, all drivers, firmware, hardware, root, all processes and services running as root, and all programs with s-uid root privileges.

A1	Verified Protection (formal methods)
B1, B2, B3	Mandatory Protection
C1, C2	Discretionary Protection
D	Minimal Security

2) Bell-LaPadula Confidentiality Model

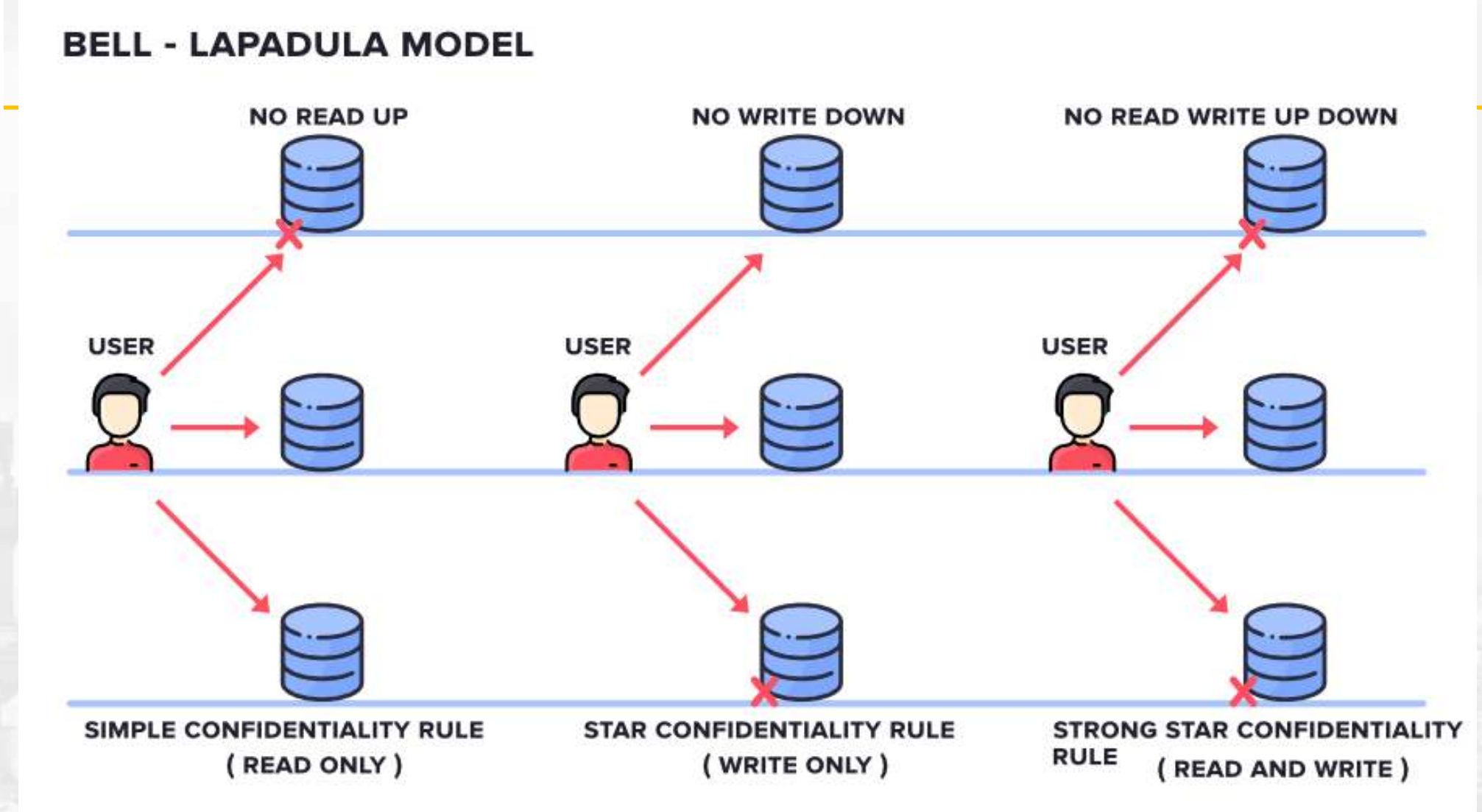
- Funded by the U.S. government, Bell-LaPadula model is the first mathematical model of a multilevel security policy. Is a state machine model that enforce the confidentiality aspects of access control, but not with integrity or availability.
- It protects information from unauthorized access.
- A subject has a security **clearance**
- An object has a security **classification**
- Is an information flow security model as it ensures information does not flow in an insecure manner.
- All mandatory access control (MAC) model are based on the Bell-LaPadula model.

- The Simple Security Property (ss Property) states that a subject at a given security level cannot read data that resides at a higher security level. (No Read Up).
- The * (star) Security Property states that a subject in a given security level cannot write information to a lower security level. (No Write Down).
- The Strong Star Property states that a subject that has read and write capabilities can only perform those functions at the same security level, nothing higher and nothing lower. A subject to be able to read and write to an object, the clearance and classification must be equal.

A BLP Example

Security level	*Subject*	*Object*
Top Secret	Tamara	Personnel Files
Secret	Samuel	E-Mail Files
Confidential	Claire	Activity Logs
Unclassified	James	Telephone Lists

- Tamara can read all files
- Claire cannot read Personnel or E-Mail Files
- James can only read Telephone Lists


BELL - LAPADULA MODEL
NO READ UP
NO WRITE DOWN
NO READ WRITE UP DOWN
USER
USER
USER
SIMPLE CONFIDENTIALITY RULE
(READ ONLY)
STAR CONFIDENTIALITY RULE
(WRITE ONLY)
STRONG STAR CONFIDENTIALITY RULE
(READ AND WRITE)

Bell–LaPadula: Military Information Enrichment

Simple Security Property:
- No read up

★-property:
- No write down
- Confinement property

High-quality, high-value, accurate information in a secure environment

No declassification of high-value information

Combining and validating information, enriching, enhancing its value

Selectively and purposefully provide very limited information and give commands (with common sense)

Large amount of low-grade, inaccurate information in an insecure environment

3) Biba Integrity Model

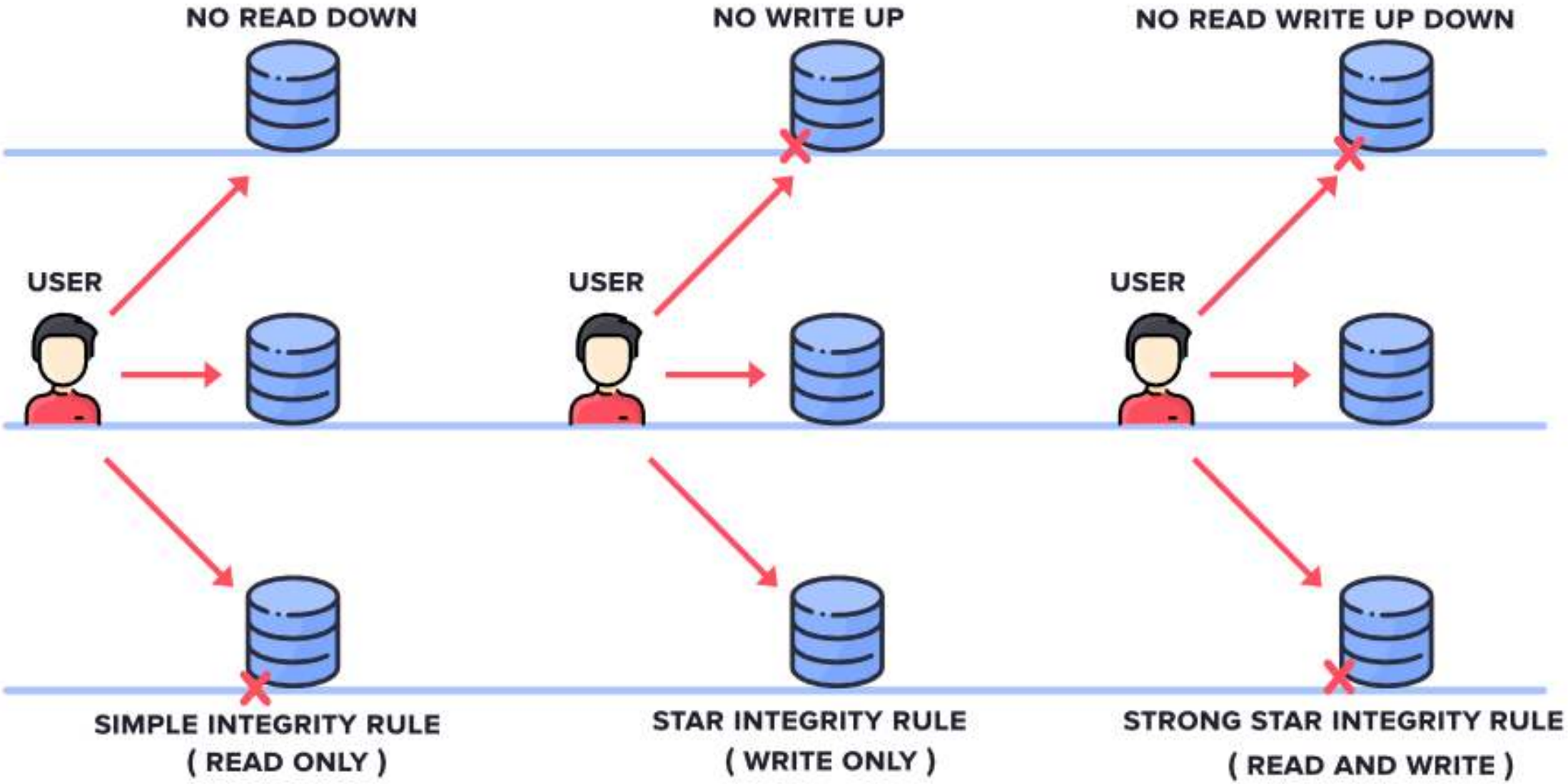
Similar to Bell-LaPadula

- Provides access controls to ensure that objects or subjects **cannot have less integrity** as a result of read/write operations
- Ensures no information from a subject can be passed on to an object in a higher security level
  - This prevents infecting data of higher integrity with data of lower integrity

What is an example of a piece of data that needs high integrity, but no confidentiality?

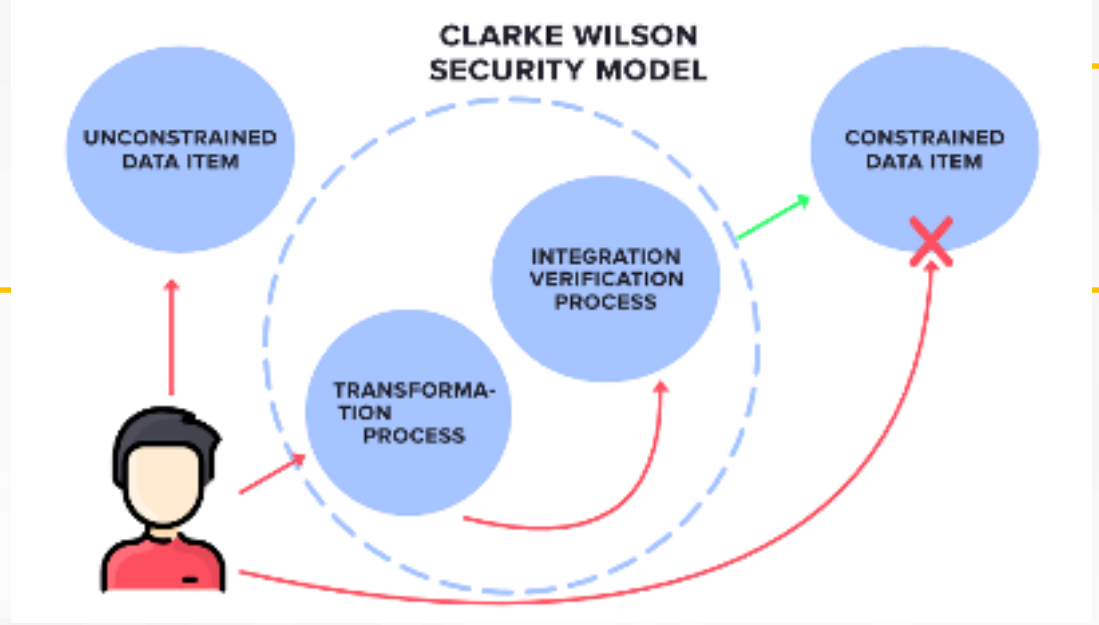
- Assigns integrity levels to subjects and objects using two properties
  - The simple integrity (read) property – No Read Down
    - A subject cannot write data to an object at a higher integrity level
  - The integrity * (write) property - No Write Up
    - A subject cannot read data from a lower integrity level

BIBA MODEL


NO READ DOWN
NO WRITE UP
NO READ WRITE UP DOWN
USER
USER
USER
SIMPLE INTEGRITY RULE
(READ ONLY)
STAR INTEGRITY RULE
(WRITE ONLY)
STRONG STAR INTEGRITY RULE
(READ AND WRITE)

4) Clark-Wilson Integrity Model

- Built upon principles of **change control** rather than integrity levels
- Designed for the commercial environment
- Its change control principles
  - No changes by unauthorized subjects
  - No unauthorized changes by authorized subjects
  - The maintenance of internal and external consistency
- Works with “Separation of duties”.
- Policy defined in terms of access triples <userID, TP, {CDIs}>



- Clark-Wilson focuses on how to ensure that programs can be trusted
- The policy is constructed in terms of the following categories:
  - Constrained Data Items: CDIs are the objects whose integrity is protected, can be manipulated by TPs.
  - Unconstrained Data Items: UDIs are objects not covered by the integrity policy, can be manipulated by users via primitive read and write operations.
  - Transformation Procedures: Here, the Subject's request to access the Constrained Data Items is handled by the Transformation process which then converts it into permissions and then forwards it to Integration Verification Process.
  - Integrity Verification Procedures: The Integration Verification Process will perform Authentication and Authorization. If that is successful, then the Subject is given access to Constrained Data Items.

5) Graham-Denning Access Control Model

- It is a computer security model that shows how subjects and objects should be securely created and deleted. It also addresses how to assign specific access rights.
- It is mainly used in access control mechanisms for distributed systems.
- Composed of three parts
  - A set of objects O
  - A set of subjects S
    - The domain is the set of constraints controlling how subjects may access objects
  - A set of rights R
- This model addresses the security issues associated with how to define a set of basic rights on how specific subjects can execute security functions on an object.
- **Primitive protection rights**
  - Create or delete object, create or delete subject
  - Read, grant, transfer and delete access rights

Graham-Denning Access Control Model

The model has eight basic protection **rules** (actions) that outline:

- How to securely create an object.
- How to securely create a subject.
- How to securely delete an object.
- How to securely delete a subject.
- How to securely provide the read access right.
- How to securely provide the grant access right.
- How to securely provide the delete access right.
- How to securely provide the transfer access right.

6) Harrison-Ruzzo-Ullman Model

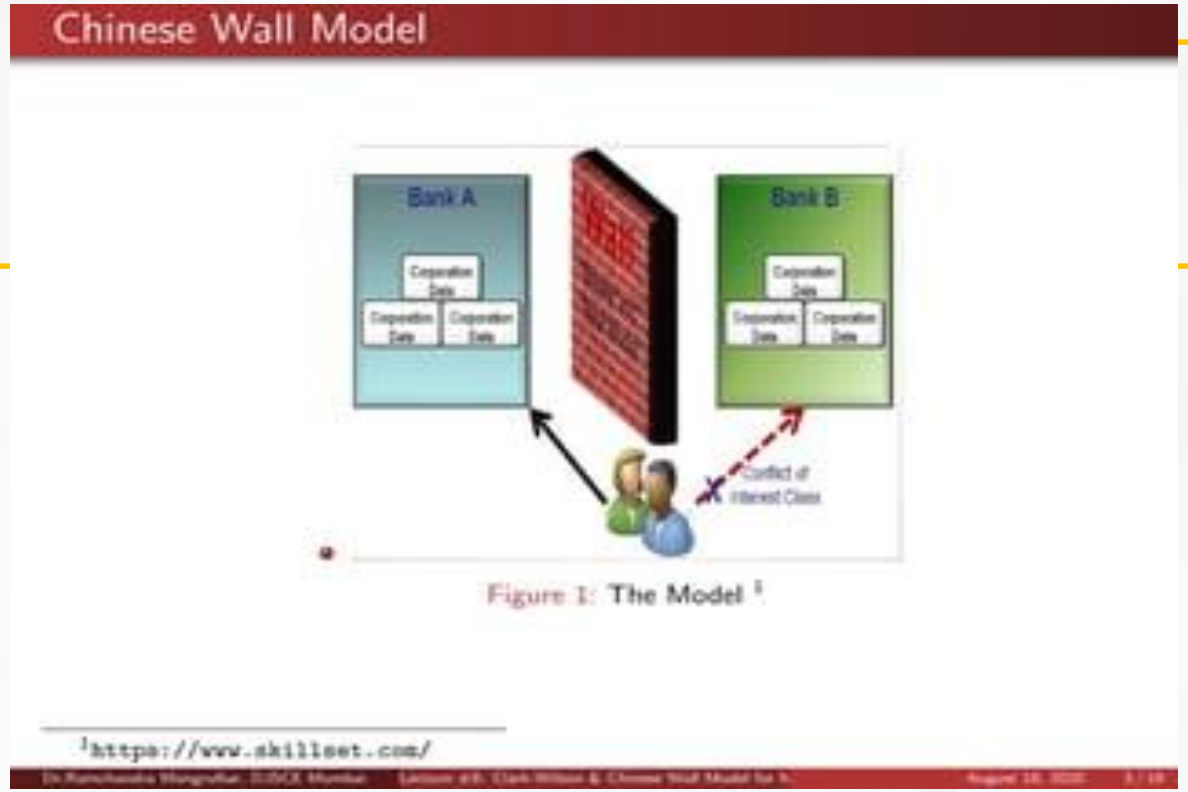
- A variation on Graham- Denning model.
- Defines a method to **allow changes to access rights and the addition and removal** of subjects and objects
  - A process that the Bell-LaPadula model does not have
  - Since systems change over time, their protective states need to change
- Built on an access control matrix
- Includes a set of generic rights and a specific set of commands.
- Used to answer the following type of questions
  - Will user X ever have access to object Y?

Harrison, Ruzzon, Ullman (HRU) Access Control Model

- Difference from G-D Model
  - Create object o
  - Create subject s
  - Destroy subject s
  - Destroy object o
  - Enter right r into A[s,o]
  - Delete right r from A[s,o]

7) Brewer-Nash Model (Chinese Wall)

- Also known as a Chinese Wall
- A model that allows for dynamically changing access controls that protect against conflicts of interest
- 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.
- The modification of access control policies is based on the behavior of users. This means that if a user who has access to the data is on the other side, they cannot access data from the other side or are unavailable to the same user.



- As an example, imagine that your security firm does security work for many large firms. If one of your employees could access information about all the firms that your company has worked for, he might be able to use this data in an unauthorized way. Therefore, the Chinese Wall model would prevent a worker consulting for one firm from accessing data belonging to another, thereby preventing any COI.

SECURITY MANAGEMENT MODEL

1) ISO 27000 Series

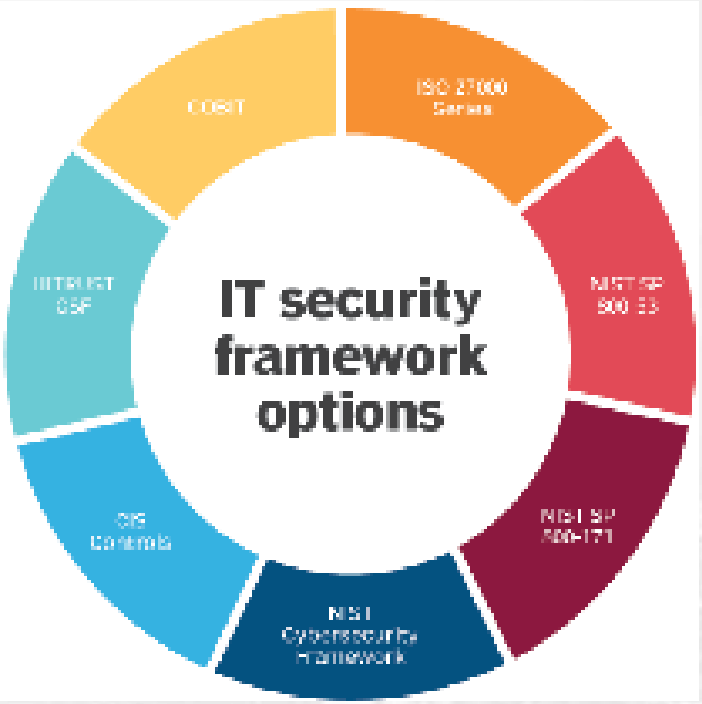
2) NIST Security Model

3) COBIT (Control Objectives for Information and Related Technology)

4) COSO (Committee Of Sponsoring Organizations of the Tread way Commission)

5) ITIL (Information Technology Infrastructure Library)

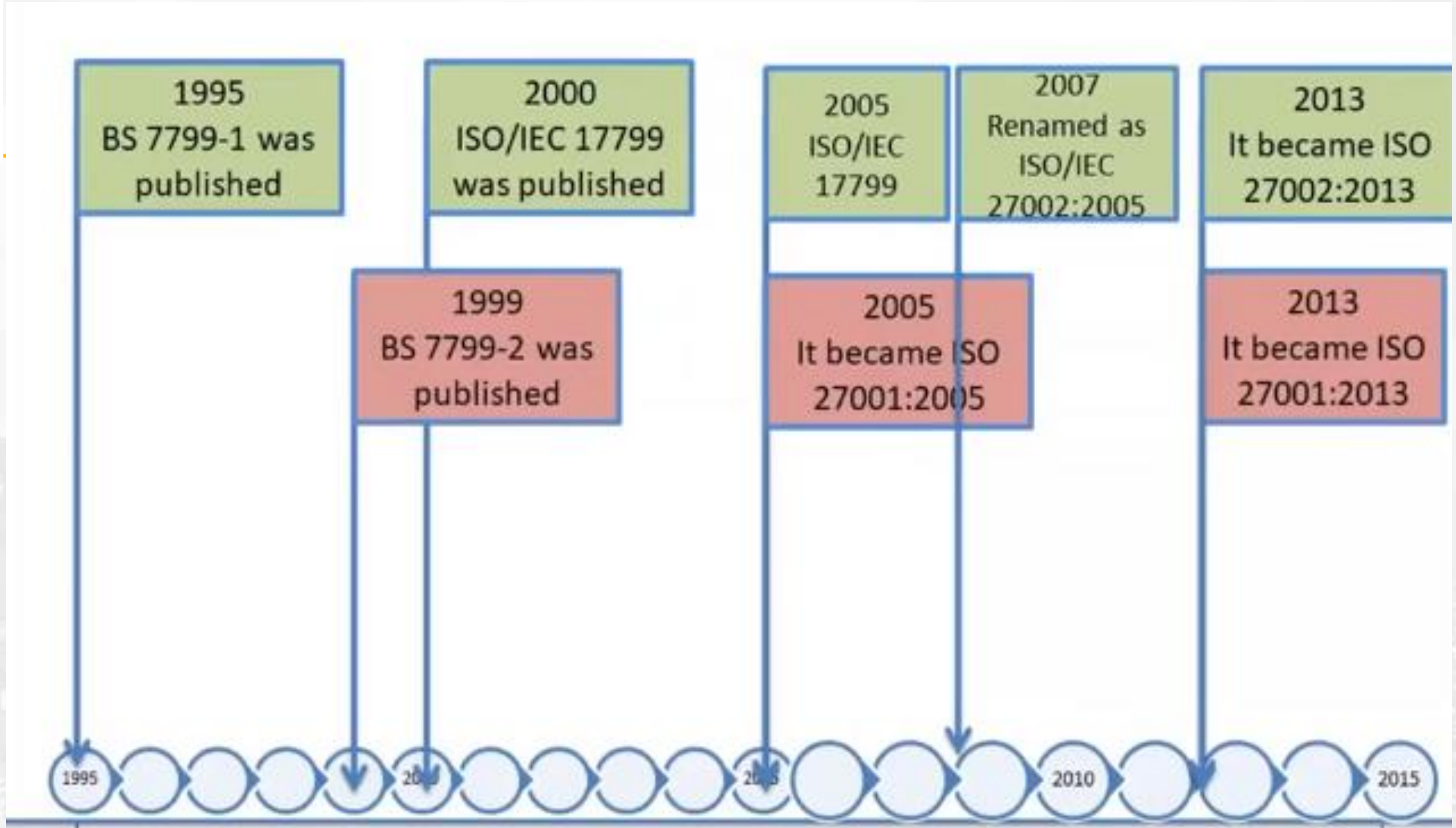
6) ISGF (Information Security Governance Framework)



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 then later as ISO/IEC 17799.
  - Since been renamed ISO/IEC 27002.
- Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission, the ISO/IEC 27000 series is comprised of over a dozen standards designed to help organizations improve their information technology security by building a strong information security management system (ISMS).
- An ISMS implemented according to these standards is designed to mitigate risk across three pillars of information security: people, processes, and technology.
- Establishes guidelines for initiating, implementing, maintaining, and improving information security management .

- The ISO 27000 family of standards is designed to certify a company's information security policies.
- ISO 27000 provides an overview of information security management systems as well as terms and definitions commonly used in the other standards in the ISO/IEC 27000 family. It also explains each standards' scope, roles, function, and relationship to each other.
- The ISO 27000 family of standards is broad in scope and is applicable to organizations of all sizes and in all sectors. As technology continually evolves, new standards are developed to address the changing requirements of information security in different industries and environments.
- ISO 27000 outlines the security techniques necessary to properly safeguard customer data. ISO 27001 is where those principles meet the real world. Businesses implement the requirements outlined in ISO 27000 standards and verify the effectiveness of their ISMS through an ISO 27001 audit.


1995
BS 7799-1 was published
2000
ISO/IEC 17799 was published
2005
ISO/IEC 17799
2007
Renamed as ISO/IEC 27002:2005
2013
It became ISO 27002:2013
1999
BS 7799-2 was published
2005
It became ISO 27001:2005
2013
It became ISO 27001:2013
1995
2010
2015

MIT-WPU

॥ विद्यानिर्मुक्तं सुखम् ॥

ISO 45001 and related standards — Occupational health and safety

Reduce workplace risks and make sure that everyone gets home safely with ISO 45001.

ISO 8601 — Date and time format

ISO 8601 is the internationally accepted way to represent dates and times.

ISO 6 — Camera film speed

One of the earliest ISO standards, ISO 6 allowed photographers to select the right film for their subject.

ISO 13485 — Medical devices

Manage quality throughout the life cycle of a medical device with ISO 13485.

ISO 31000 — Risk management

Manage the risks that could jeopardize your company's performance with this ISO standard.

ISO 50001 — Energy management

ISO's standard for helping organizations manage their energy performance.

ISO 639 — Language codes

Describe languages in an internationally accepted way with this standard.

ISO 9660 — ISO images for computer files

The standard that enabled Compact Discs.

ISO 14001 and related standards — Environmental management

Improve your environmental performance with this family of standards.

ISO 22000 — Food safety management

Inspire confidence in your food products with this family of standards.

ISO 37001 — Anti-bribery management systems

Prevent, detect and address bribery.

ISO 20121 — Sustainable events

Manage the social, economic and environmental impacts of your event with this standard.

ISO 4217 — Currency codes

Avoid confusion when referring to world currencies with this standard.

ISO 13216 — ISOFIX child seats for cars

ISOFIX child seats for cars with ISO 13216.

ISO/IEC 17025 — Testing and calibration laboratories

Testing and calibration performed using standard methods, non-standard methods, and laboratory-developed methods

ISO 26000 — Social responsibility

Help your organization to operate in a socially responsible way with this standard.

ISO 3166 — Country Codes

Avoid confusion when referring to countries and their subdivisions with this standard.

ISO 9001:2015

Quality management systems

The ISO 9000 family is the world's most best-known quality management standard for companies and organizations of any size.

ISO/IEC 27001:2022

Information security, cybersecurity and privacy protection

Information security management systems – Requirements

ISO 14001:2015

Environmental management systems

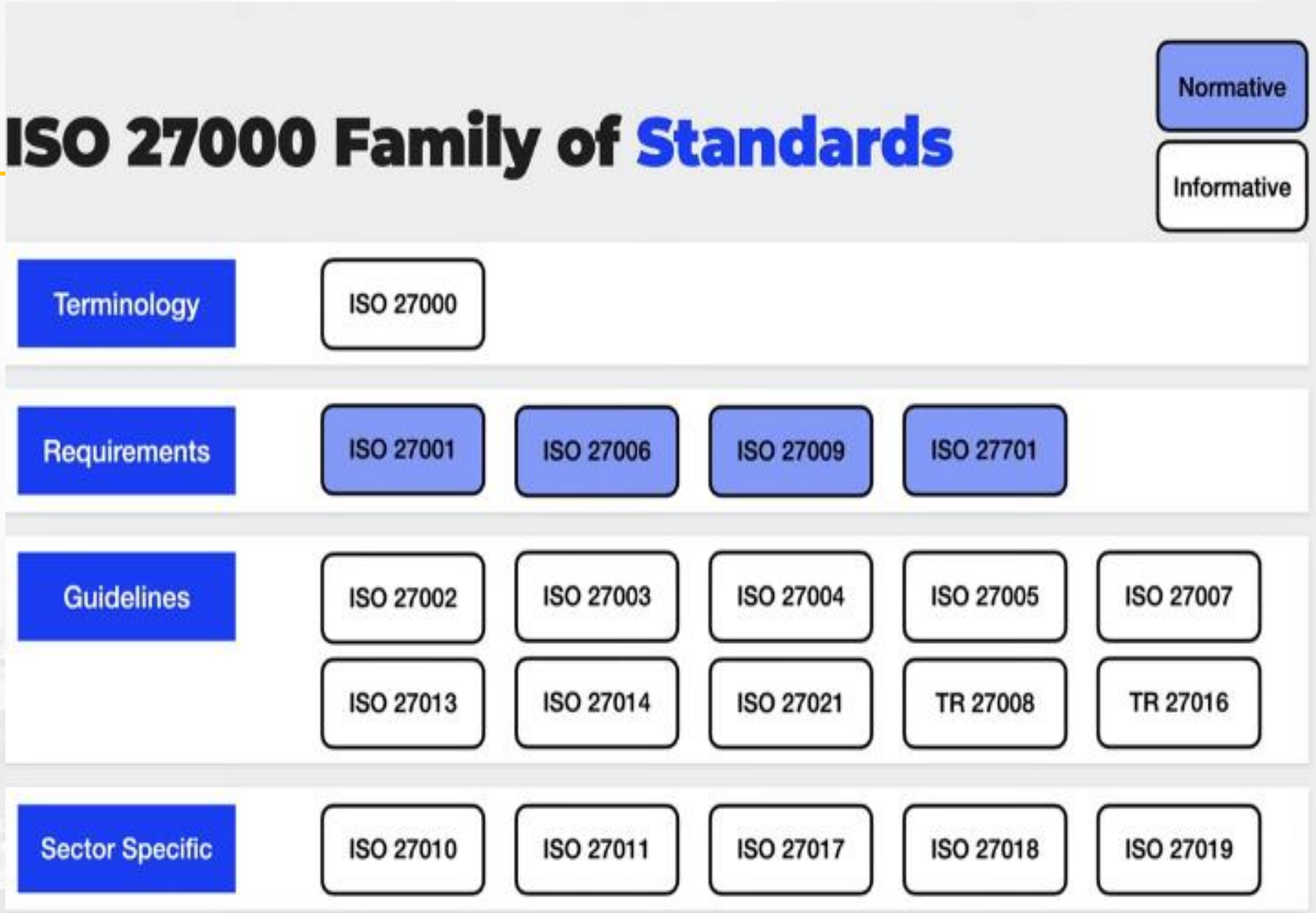
Improve your environmental performance with this family of standards.

Information technology – Security Techniques – Information security management.

Requirements for bodies providing audit and certification of information security management systems

Internal document for the committee developing sector/industry-specific versions or implementation guidelines for the ISO27K standards.

Data privacy extension to ISO 27001



ISO information security management system

- An information security management system is the entire set of information assets, systems, technologies, people, partners, processes, and policies that an organization uses to protect sensitive data. An ISMS should protect information assets from unauthorized access, proactively identify and mitigate risk, and ensure data availability.

How does ISMS protect data?

- Identifies information assets that need to be protected.
- Identifies risks to those information assets.
- Create controls to mitigate risks and protect information assets.
- Establishes a clear plan of action in the event of a data breach, including individuals responsible for each step.
- Defines a process for continually reviewing and improving the ISMS.

Plan-Do-Check-Act of BS7799:2

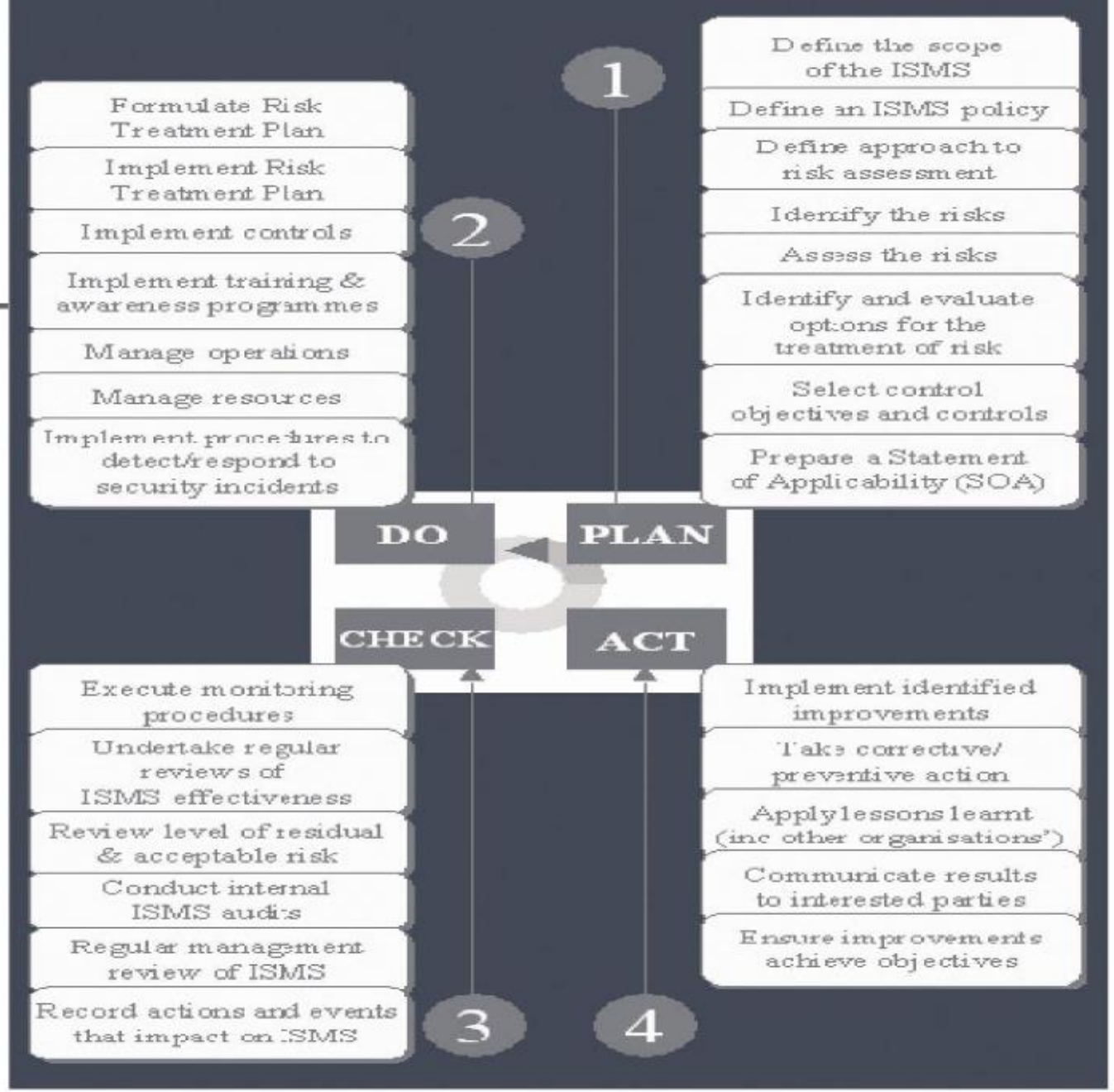


FIGURE 6-2 Plan-Do-Check-Act Cycle from BS 7799:2

What are Risks in a project?

- Risks are potential problems that may affect successful completion of a software project.
- Risks involve uncertainty and potential losses.
- Risk analysis and management are intended to help a software team understand and manage uncertainty during the development process.

Risk Analysis

Analysis of risks in project has four steps :

1. Risk identification
2. Risk projection
   - impact and likelihood of risk actually happening
3. Risk assessment
   - what will change if risk becomes problem
4. Risk management

1. Risk Identification -Types of Software Risks

1. Project risks
   - Risks that threaten the project plan
2. Technical risks
   - Risks that threaten product quality and the timeliness of the schedule
3. Business risks
   - Risks that threaten the viability of the software to be built (market risks, strategic risks, management risks, budget risks)
4. Product-specific risks
   - Risks that are specific to the product and may affect the project plan. Scope of project software are examined to identify such risks.
5. Generic risks
   - Risks that are potential threats to every software product
     - product size
     - customer characteristics
     - development environment
     - technology to be built

2. Risk Projection

- Each risk component are
  - classified according to their impact category

- Risk impact (On scale of 1 to 4) severity
  - Negligible-1
  - Marginal-2
  - Critical-3
  - Catastrophic-4

3. Risk Assessment

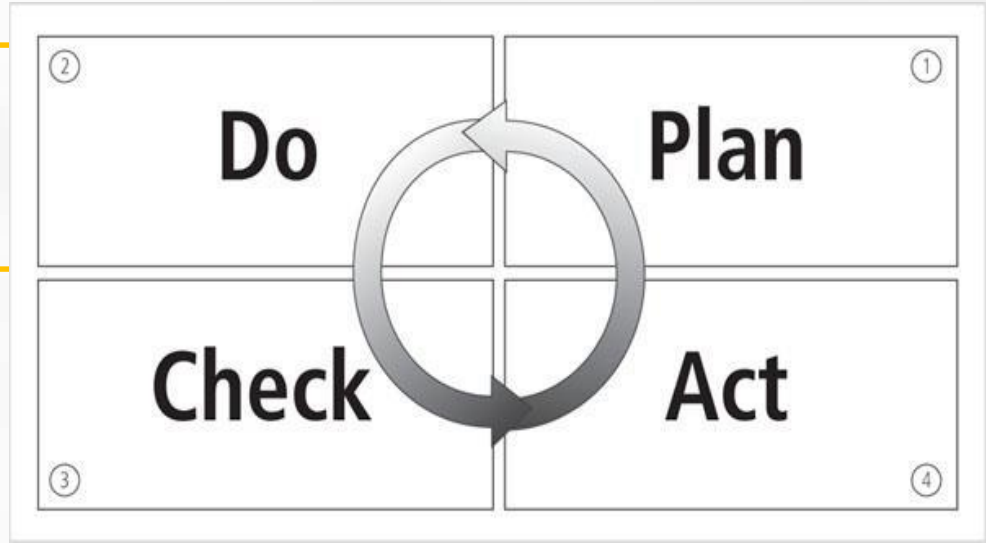
- Is likelihood of the risk occurring.
- It has two steps :
  - Risk Analysis
  - Risk Prioritization
- Based on the degree of impact, possessed by each risk, they are being assigned severity levels, namely 'High', 'Medium' and 'low'. (Priority)
- And based on their severity, they are prioritize i.e. High risks are considered as top priority whereas the low risk is regarded for the bottom most priority

4. Risk Management

- A risk management strategy can be organized into a separate Risk Mitigation, Monitoring and Management Plan.
  - Mitigation : is the process of developing options and actions to reduce threats to project objectives
  - Monitoring : project manager monitors factors that may provide an indication of whether a risk is becoming more or less likely
  - Management : assume that mitigation efforts have failed and that the risk has become a reality

RISK TABLE

Risk	Risk Type	Probability of Occurrence of Risk	Impact	Priority	Risk Management RMMM	Plan
Embedded software for XYZ system	Technical risk	60%	3- Critical	High	Monitoring : Scheduled milestone reviews with hardware group	Modification of testing strategy to accommodate delay using software simulation
HR dept is moving to a new site	Business Risks	75%	1- Negligible	Low	Mitigation	Keep alternate resource persons ready who are willing to move to a small town



- ISO/IEC 27001:2005

- The InfoSec Management System - Plan

1. Define the scope of the ISMS
2. Define an ISMS policy
3. Define the approach to risk assessment
4. Identify the risks
5. Assess the risks
6. Identify and evaluate options for the treatment of risk
7. Select control objectives and controls
8. Prepare a statement of applicability (SOA)

- **The InfoSec Management System - Do**

  9. Formulate a risk treatment plan
  10. Implement the risk treatment plan
  11. Implement controls
  12. Implement training and awareness programs
  13. Manage operations
  14. Manage resources
  15. Implement procedures to detect and respond to security incidents

- **The InfoSec Management System - Check**
  16. Execute monitoring procedures
  17. Undertake regular reviews of ISMS effectiveness
  18. Review the level of residual and acceptable risk
  19. Conduct internal ISMS audits
  20. Undertake regular management review of the ISMS
  21. Record actions and events that impact an ISMS

- **The InfoSec Management System - Act**

22. Implement identified improvements
23. Take corrective or preventive action
24. Apply lessons learned
25. Communicate results to interested parties
26. Ensure improvements achieve objectives

NIST Security Models

- NIST is the **National Institute of Standards and Technology** at the U.S. Department of Commerce.
- The NIST Cybersecurity Framework (NIST CSF) consists of standards, guidelines, and best practices that help organizations improve their **management of cybersecurity risk.**
- The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data.
- The Framework is voluntary. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection.
- The NIST CSF is designed to be flexible enough to integrate with the existing security processes within any organization, in any industry. It provides an excellent starting point for implementing information security and cybersecurity risk management in virtually any private sector organization in the United States.

- On February 12, 2013, Executive Order (EO) 13636—**"Improving Critical Infrastructure Cybersecurity"**—was issued. This began NIST's work with the U.S. private sector to "**identify existing voluntary consensus standards and industry best practices to build them into a Cybersecurity Framework.**" The result of this collaboration was the NIST Cybersecurity Framework Version 1.0.
- NIST Cybersecurity Framework includes functions, categories, subcategories, and informative references.
- Functions give a general overview of security protocols of best practices. Functions are not intended to be procedural steps but are to be performed "**concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk**." Categories and subcategories provide more concrete action plans for specific departments or processes within an organization.

https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters

5 Core Functions of NIST Cybersecurity Framework

Capability	Description
Identify	What processes and assets need protection?
Protect	Implement appropriate safeguards to ensure protection of the enterprise's assets
Detect	Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents
Respond	Develop techniques to contain the impacts of cybersecurity events
Recover	Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events

IDENTIFY

The Identify function is focused on laying the groundwork for an effective cybersecurity program. This function assists in developing an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. To enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs, this function stressed the importance of understanding the business context, the resources that support critical functions, and the related cybersecurity risks.

Essential activities in this group include:

- Identifying physical and software assets to establish the basis of an asset management program
- Identifying the organization's business environment including its role in the supply chain
- Identifying established cybersecurity policies to define the governance program as well as identifying legal and regulatory requirements regarding the cybersecurity capabilities of the organization
- Identifying asset vulnerabilities, threats to internal and external organizational resources, and risk response activities to assess risk
- Establishing a risk management strategy
- Identifying a supply chain risk management strategy including priorities, constraints, risk tolerances, and assumptions used to support risk decisions associated with managing supply chain risks

PROTECT

The Protect function outlines appropriate safeguards to ensure delivery of critical infrastructure services and supports the ability to limit or contain the impact of a potential cybersecurity event.

Critical activities in this group include:

- Implementing protections for Identity Management and Access Control within the organization including physical and remote access
- Empowering staff through security awareness training including role based and privileged user training
- Establishing data security protection consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information
- Implementing processes and procedures to maintain and manage the protections of information systems and assets
- Protecting organizational resources through maintenance, including remote maintenance activities
- Managing technology to ensure the security and resilience of systems, consistent with organizational policies, procedures, and agreements

DETECT

Detecting potential cybersecurity incidents is critical and this function defines the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner.

Activities in this function include:

- Ensuring anomalies and events are detected, and their potential impact is understood
- Implementing continuous monitoring capabilities to monitor cybersecurity events and verify the effectiveness of protective measures including network and physical activities

RESPOND

The Respond function focuses on appropriate activities to take action in case of a detected cybersecurity incident and supports the ability to contain the impact of a potential cybersecurity incident.

The essential activities for this function include:

- Ensuring response planning process are executed during and after an incident
- Managing communications with internal and external stakeholders during and after an event
- Analyzing the incident to ensure effective response and supporting recovery activities including forensic analysis and determining the impact of incidents
- Performing mitigation activities to prevent expansion of an event and to resolve the incident
- Implementing improvements by incorporating lessons learned from current and previous detection / response activities

RECOVER

The Recover function identifies appropriate activities to renew and maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. Timely recovery to normal operations is impressed upon, to reduce the impact from a cybersecurity incident.

Essential activities for this function somewhat overlap with those of Respond and include:

- Ensuring the organization implements recovery planning processes and procedures to restore systems and/or assets affected by cybersecurity incidents
- Implementing improvements based on lessons learned and reviews of existing strategies
- Internal and external communications are coordinated during and following the recovery from a cybersecurity incident

Function

GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy

Function

IDENTIFY (ID): Help determine the current cybersecurity risk to the organization

Function

PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk

Function

DETECT (DE): Find and analyze possible cybersecurity attacks and compromises

Function

RESPOND (RS): Take action regarding a detected cybersecurity incident

Function

RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident

https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Source= nist.gov

Why should I use the NIST Cybersecurity Framework?

First, let's take a step back and list the cybersecurity issues that are probably top of mind.

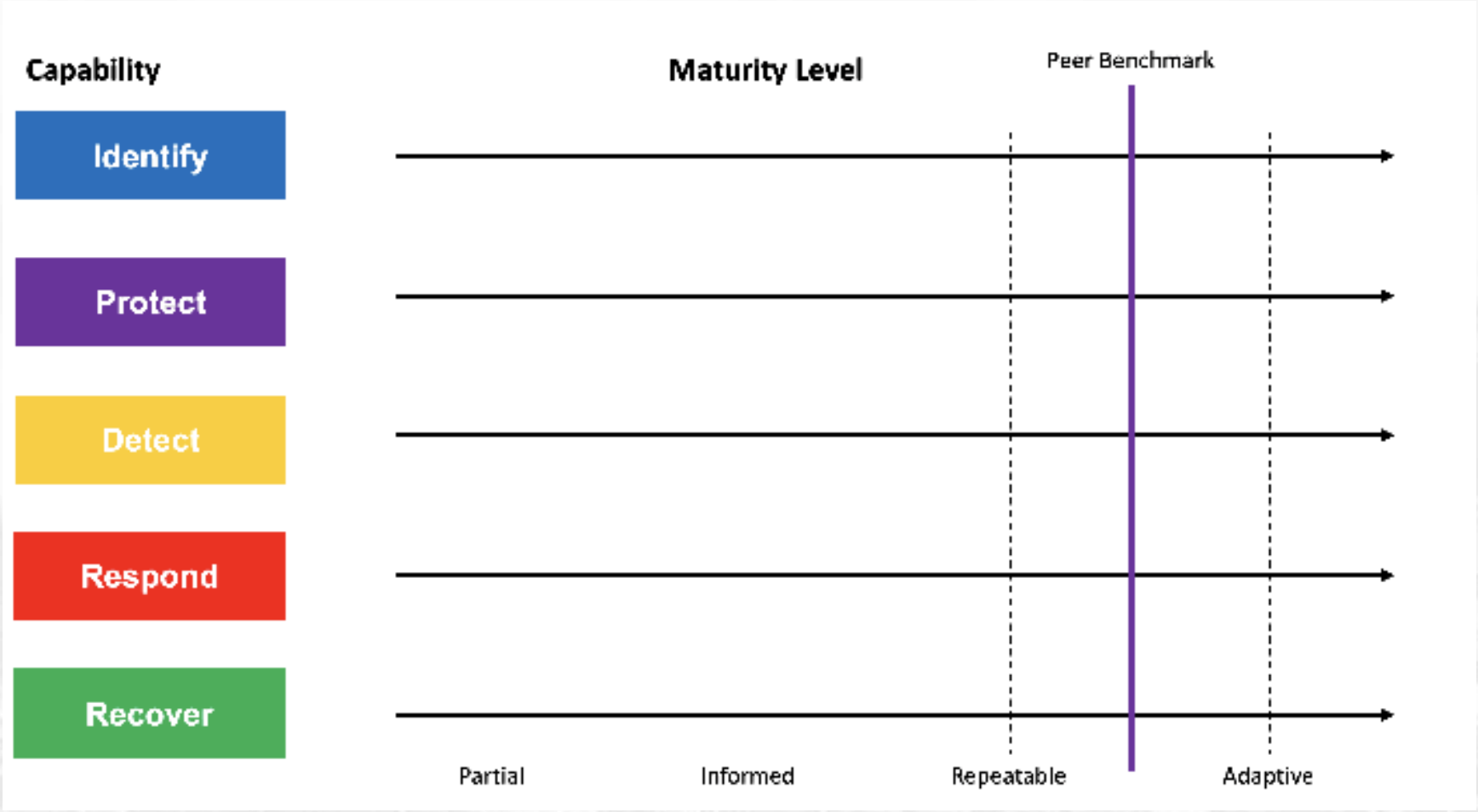
1. You worry about unseen risks and vulnerabilities.
2. You do not have an accurate inventory of assets that need to be protected.
3. Your team spends much effort chasing items that will not have impact, while you would like them to focus on real risk
4. You want to know how to address risk items given your current tools and what's available in the marketplace
5. Your colleagues outside the security team do not understand cyber risk and therefore fail to "own" critical mitigation tasks
6. Your board is beginning to ask you about quantifying the risk reduction outcomes from the strategic cybersecurity plan that your team has been executing. "Are we compliant with NIST"?

- The framework can help you with these challenges. You will be able to leverage the learnings of people who have successfully addressed similar problems.
- The objective of the framework is to help you prioritize cybersecurity investments and decisions. The framework also helps you reason about the maturity of your program and provides a framework for conversations with stakeholders including your senior management and your board of directors

How to get started with NIST Cybersecurity Framework

- Aligning with the framework means enumerating all your activities and labelling these elements with one of these 5 function labels.
- For example, the Identify label will be for tools that help you inventory your assets. Tools like Firewalls and Crowdstrike will go into Protect. However, depending on their capabilities you would also put them in Detect along with your IDS and SIEM. Your incident response tools and playbooks go into Respond. Your backup and recovery tools are part of Recover.

Understanding Maturity Levels in NIST Language



- **Tier 1 – Partial:** The organization is familiar with the NIST CSF and may have implemented some aspects of control in some areas of the infrastructure. Implementation of cybersecurity activities and protocols has been reactive vs. planned. The organization has limited awareness of cybersecurity risks and lacks the processes and resources to enable information security.

- **Tier 2 – Risk Informed:** The organization is more aware of cybersecurity risks and shares information on an informal basis. It lacks a planned, repeatable, and proactive organization-wide cybersecurity risk management process.

- **Tier 3 – Repeatable:** The organization and its senior executives are aware of cybersecurity risks. They have implemented a repeatable, organization-wide cybersecurity risk management plan. The cybersecurity team has created an action plan to monitor and respond effectively to cyberattacks.

- **Tier 4 – Adaptive:** The organization is now cyber resilient and uses lessons learned and predictive indicators to prevent cyberattacks. The cybersecurity team continuously improves and advances the organization's cybersecurity technologies and practices and adapts to changes in threats quickly and efficiently. There is an organization-wide approach to information security risk management with risk informed decision-making, policies, procedures, and processes. Adaptive organizations incorporate cybersecurity risk management into budget decisions and organizational culture.

Control Objectives for Information and Related Technology (COBIT)

– Created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992

– This framework is mainly focused on business and defines the generic process for IT management.

– COBIT's focus is on making IT so simplified that IT professionals, auditors, and business executives, coming from every background, can understand it, control it, predict the outcomes, and set the goals.

– It helped to reduce the risk from IT implementations.

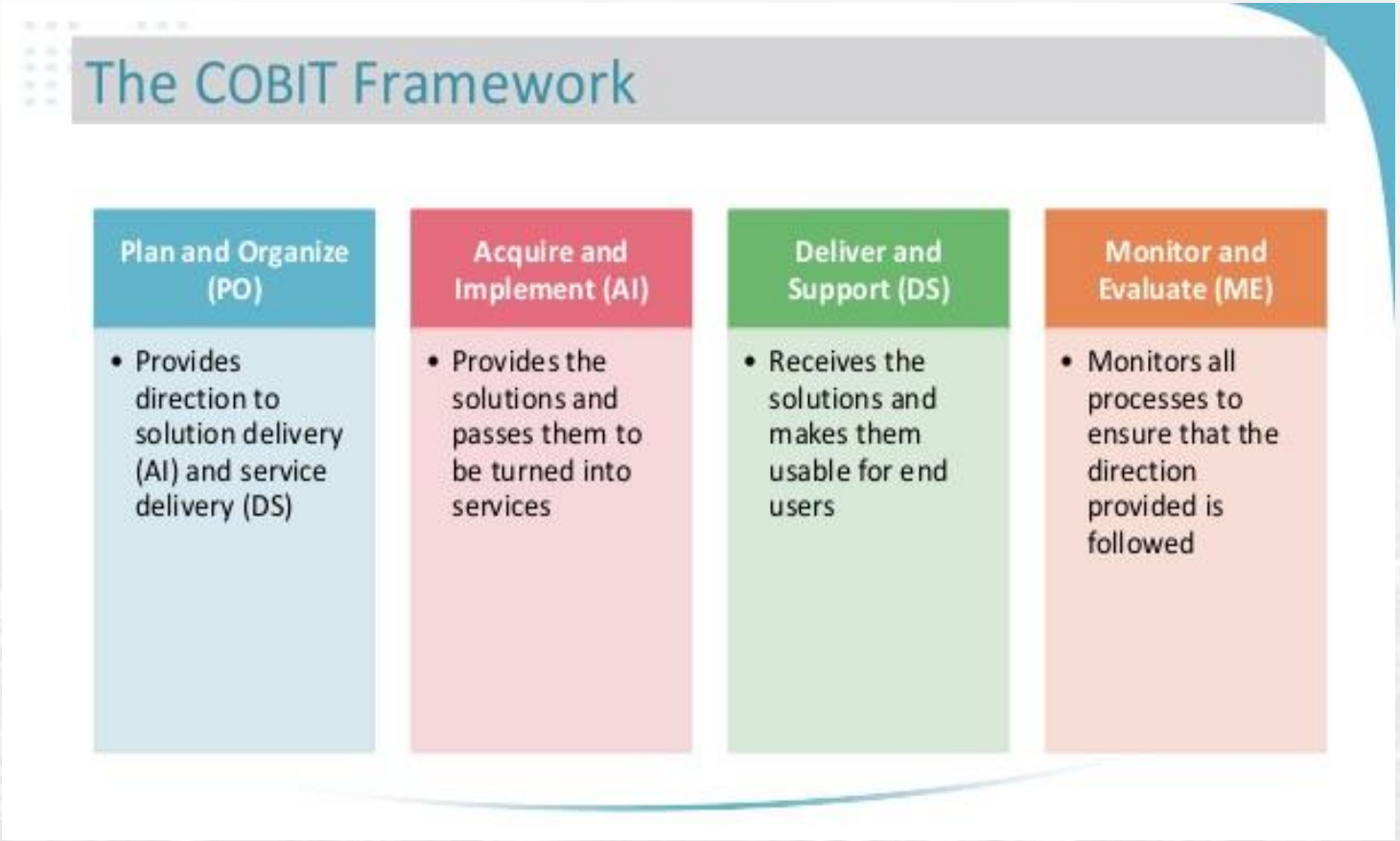
COBIT is business orientation, which links the business goals with the available resources by providing various metrics used to measure the business's success.

COBIT is based on five key principles for IT enterprise governance:

- 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

– Objectives categorized into four domains:

- Plan and organize
- Acquire and implement
- Deliver and support
- Monitor and evaluate



- Plan and organize
  - –Makes recommendations for achieving organizational goals and objectives through the use of IT
- Acquire and implement
  - –Focuses on specification of requirements
  - –Acquisition of needed components
  - –Examines ongoing maintenance and change requirements

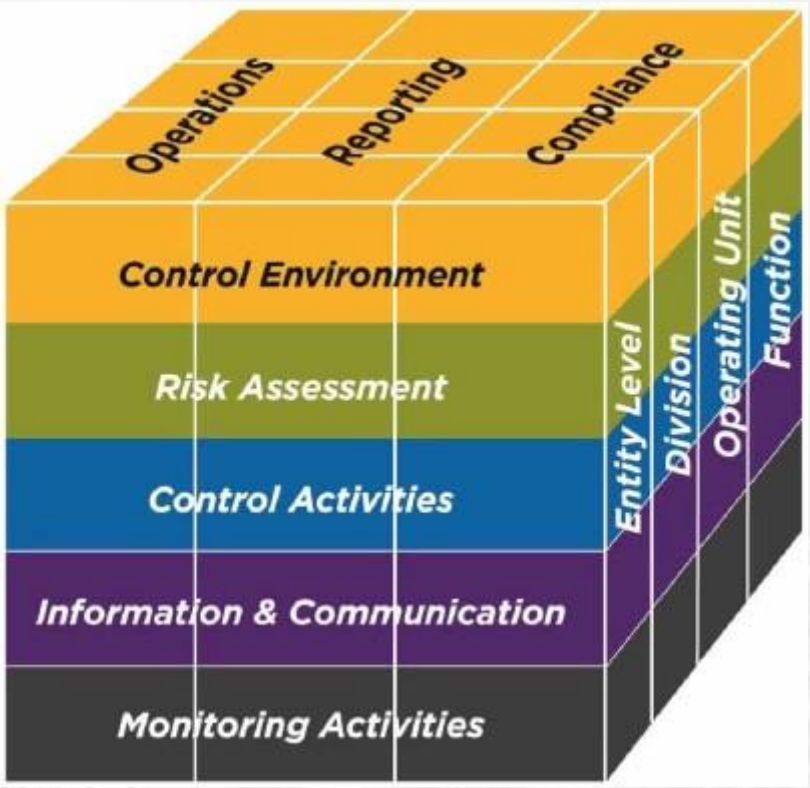
- Delivery and support
  - –Focuses on the functionality of the system and its use to the end user
  - –Examines systems applications: including input, processing, and output components
  - –Examines processes for efficiency and effective of operations
- Monitor and evaluate
  - –Seeks to examine the alignment between IT systems usage and organizational strategy
  - –Identifies the regulatory requirements for which controls are needed
  - –Monitors the effectiveness and efficiency of IT systems against the organizational control processes in the delivery and support domain

COSO

A U.S. private-sector initiative

- The COSO Framework is a system used to establish internal controls to be integrated into business processes. Collectively, these controls provide reasonable assurance that the organization is operating ethically, transparently and in accordance with established industry standards.
- COSO is an acronym for the Committee of Sponsoring Organizations.
- Its major objective is to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence
- Has established a common definition of internal controls, standards and criteria.

- Built on five interrelated components:
  - –Control environment
  - –Risk assessment
  - –Control activities
  - –Information and communication
  - –Monitoring



Information Technology Infrastructure Library (ITIL)

- A collection of methods and practices useful for managing the development and operation of information technology infrastructures
- Has been produced as a series of books
  - Each of which covers an IT management topic
- Includes a detailed description of many significant IT-related practices
  - Can be tailored to many IT organizations

Information Security Governance Framework (ISGF)

- A managerial model
  - –Provides guidance in the development and implementation of an organizational information security governance structure
- Includes recommendations for the responsibilities of members of an organization
- Recommendations for responsibilities of members of an organization
  - –Board of directors/trustees
- Provide strategic oversight for information security
  - –Senior executives
- Provide oversight of a comprehensive information security program for the entire organization
  - –Executive team members
- Oversee the organization's security policies and practices

- Provide information security for the information and information systems that support the operations and assets under their control
  - All employees and users
- Maintain security of information and information systems accessible to them

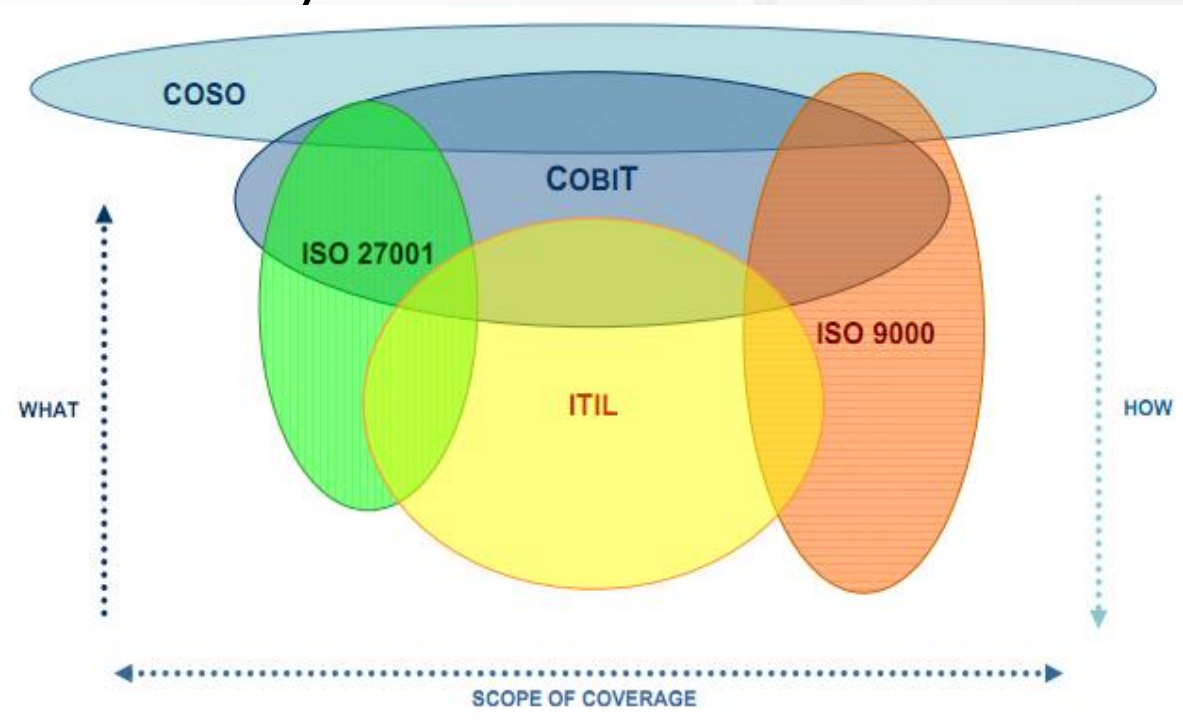
Security Management Models

–System Models (BLP, Biba, CWI, HRU, BN, etc).

–ISO 27000 Series

–NIST Models

–Others (COBIT, COSO, ITIL, Corporate Governance)



- COBIT is usually employed by business executives to successfully execute key policies and procedures. Additionally, it is often used to tie together controls, technical issues and risks within an organization.
- ITIL was originally designed for use within the U.K. government and is most applicable within that realm. However, it is now an globally accepted standard and is in-use by many companies outside the geographical area of origin.
- ISO 27002 is commonly used by or in accord with an IT department specific to the organization. The IT department is the focus of the resulting management system controls.
- NIST covers all steps in the Risk Management Framework that addresses the selection of security controls according to FIPS (Federal Information Processing Standard) 200. It is used by U.S. federal organizations to meet ISMS requirements.

Strengths

- COBIT is managed by ISACA (Information Systems Audit and Control Association) and keeps the standard up-to-date and on-par with current technology. It is a globally accepted standard and encompassed far more than just the information security scope that other standards are limited to. Accordingly, it is also easier to partially implement COBIT without requiring a full-spectrum analysis and commitment by the organization.
- ITIL is created and managed by the U.K. government, and is a natural fit for companies in that area of the world. However, the ITIL standard is used worldwide and may be considered for any company regardless of geographical location. ITIL excels at increasing visibility into and management of internal process to positively impact efficiency and economy.
- ISO 27002 is associated with a very respected and widely known standard (ISO 27001), and will be recognized and understood by those familiar with the ISO/IEC standards. This standard allows system managers to identify and mitigate gaps and overlaps in coverage.

Weaknesses

- While being widely scoped is can be viewed as a strength for COBIT, it can also be a detractor during implementation. Being by design not limited to a single area, it can often lead to gaps in coverage.
- While focused on information security only, ITIL is considered to be a higher-level standard than ISO 27002, and points to ISO standards for detailed implementation. Specific implementation details are rather lacking.
- ISO 27002 is focused specifically and purposefully on information security and is therefore limited in scope compared to other standards such as COBIT.

When to Use

- COBIT is a good candidate when an organization wishes to create an organization-wide framework for management that is scoped outside of information security only. While not providing direct accreditation, certification can be achieved through closely aligned paths.
- ITIL points to ISO standards as a framework in which to implement a solution. This applies well for organizations wishing to use ISO standards with global recognition without necessarily achieving an ISO 27001 certification.
- The associated certification for ISO 27002 (ISO 27001) provides a worldwide recognition and acceptance, and therefore organizations wishing to operation across international boundaries may find implementation and certification advantageous. Additionally, some ISO 27001 certified companies require partners to become certified as well.

What should be implemented first?

- There’s no exact answer about this question, but its really depend on your company and your requirement. Most of company start to implemented COBIT first because its cover general information system. And after that they usually choose between ITIL or ISO27001. Another consideration is about budget and authorities. COBIT implementation usually run from internal audit budget and ITIL or ISO27001 usually performed using IT department budget. This consideration usually makes what kind of standard to implemented first become depend on management policy

What is the easiest standard?

- From the implementation view, ITIL is the easiest standard to be implemented. Because, ITIL could be implemented partially and still not have impact on performance. Example, if IT department lack of budget and he could choose to implement IT Service Delivery layer only, and the next year he will try to implement IT Release Management or IT Problem Management. However COBIT and ISO27001 is quite difficult to be implemented partially, since it should see a process in bigger view first before they could implemented partially.

Tutorial 1

Summary of Security Management Models