Security Architecture

Lect 4

Questions

1) Do you conduct risk assessments?
2) Do you write policies?
3) Have you developed an information security management system?
4) Have you set up an information security governance mechanism e.g. A steering committee?
5) Have you designed security controls for systems?

➢Then you do have a security Architecture

- **Enterprise** - Multiple internal networks, internal areas or domains, and various internal devices and systems, applications, and a diverse user presence as a single collective unit.
- **Architecture** - The highest level concept of a system in its environment.
- **Security Architecture** - A high-level design used to satisfy a system's security requirements as defined in an organization's security policy
- **Enterprise Security Architecture** - Defines the information security strategy that consists of layers of policy, standards, and procedures and the way they are linked across an enterprise

- Security architecture is a set of security principles, methods, and models designed to align with your objectives and help keep your organization safe from cyber threats.
- Security architecture translates the business requirements to executable security requirements.
- Security architecture is a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment.
- It also specifies when and where to apply security controls. The design process is generally reproducible.
- In security architecture, the design principles are reported clearly, and in-depth security control specifications are generally documented in independent documents.
- System architecture can be considered a design that includes a structure and addresses the connection between the components of that structure.

Attributes of security architecture

- R**elationships and Dependencies:** Signifies the relationship between the various components inside IT architecture and the way in which they depend on each other.
- **Benefits:** The main advantage of security architecture is its standardization, which makes it affordable. Security architecture is cost-effective due to the re-use of controls described in the architecture.
- **Form:** Security architecture is associated with IT architecture; however, it may take a variety of forms. It generally includes a catalog of conventional controls in addition to relationship diagrams, principles and so on.
- **Drivers:** Security controls are determined based on four factors:
  - Risk management
  - Benchmarking and good practice
  - Financial
  - Legal and regulatory

Security architecture process

- **Architecture Risk Assessment:** Evaluates the business influence of vital business assets, and the odds and effects of vulnerabilities and security threats.
- **Security Architecture Design:** The design and architecture of security services, which facilitate business risk exposure objectives.
- **Implementation:** Security services and processes are implemented, operated and controlled. Assurance services are designed to ensure that the security policy and standards, security architecture decisions, and risk management are mirrored in the real runtime implementation.
- **Operations and Monitoring:** Day-to-day processes, such as threat and vulnerability management and threat management. Here, measures are taken to supervise and handle the operational state in addition to the depth and breadth of the systems security.

The infrastructure includes items such as:

- Hardware
- Software
- Operating System and all associated functions
- Applications
- Network environment
- Security awareness and training
- Information system security supporting policies, procedures, baselines and standards

Security models

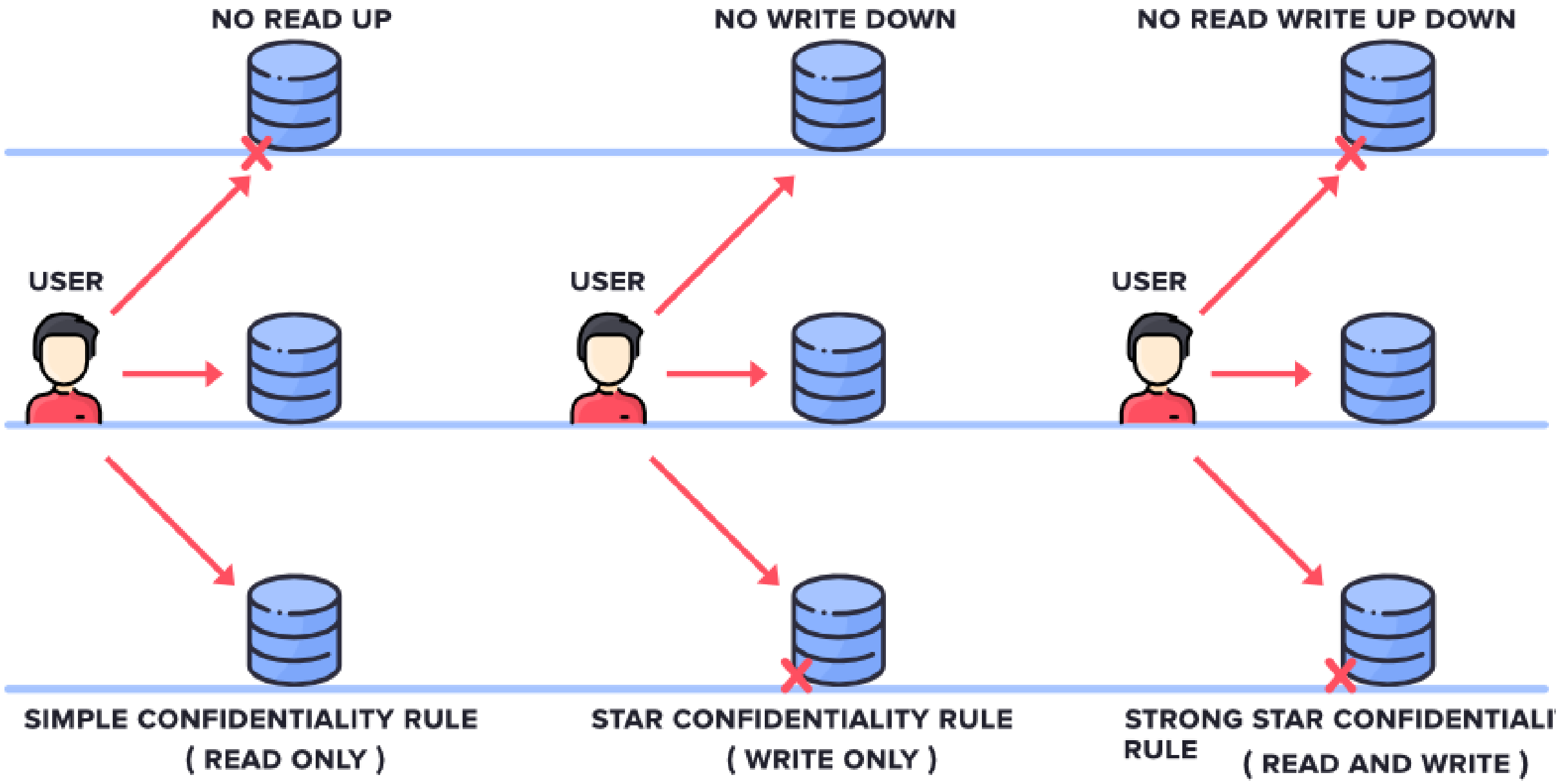
- Security models depict the essential elements of security and their relation to the operating system's performance.
- No organization can protect its sensitive data or information without having efficient and effective security models.
- It is possible to say that the principal goal of security models is to give the necessary degree of understanding required for the effective and successful implementation of essential security needs.
- **These models are utilized to achieve security goals, i.e., Confidentiality, Integrity, and Availability.**
- **Put it is a model for CIA Triad maintenance.**

- There are five major types of Classic Security Models.
  - Bell-LaPadula
  - Biba
  - Clarke Wilson Security Model
  - Brewer and Nash Model
  - Harrison Ruzzo Ullman Model

Bell-LaPadula

- The Model was created in the 1950s by Scientists David Elliot Bell and Leonard .J. LaPadula. Thus, the Model is known as Bell-LaPadula Model. This Model is used to protect the security of confidentiality. In this case, the classifications used to classify Subjects(Users) and Objects(Files) are arranged in a non-discretionary manner and about various layers of secret.
- It has three primary rules:
  - **SIMPLE CONFIDENTIALITY RULE:** The Simple Confidentiality Rule says that the Subject can read the files on the same Layer of Secrecy and the Lower Layer of Secrecy but not the Higher Layer of Secrecy because of this, this rule is known as No-Read-UP.
  - **Star Confidentiality Rule 2**: This rule stated that the Subject is only able to write the document on the same layer of secrecy but not able to write in the lower Layer of Secrecy, and that is why we called this rule a No Write-down
  - **The STRONG STAR CONFIDENTIALITY Rule:** Strong Star Confidentiality Rule is highly secure and robust that states that the Subject can read and write documents on the same Layer of Secrecy only, and not on the upper Layer of Secrecy or the Lower Layer of Secrecy This is why this rule is referred to as NO READ WRITE and DOWN

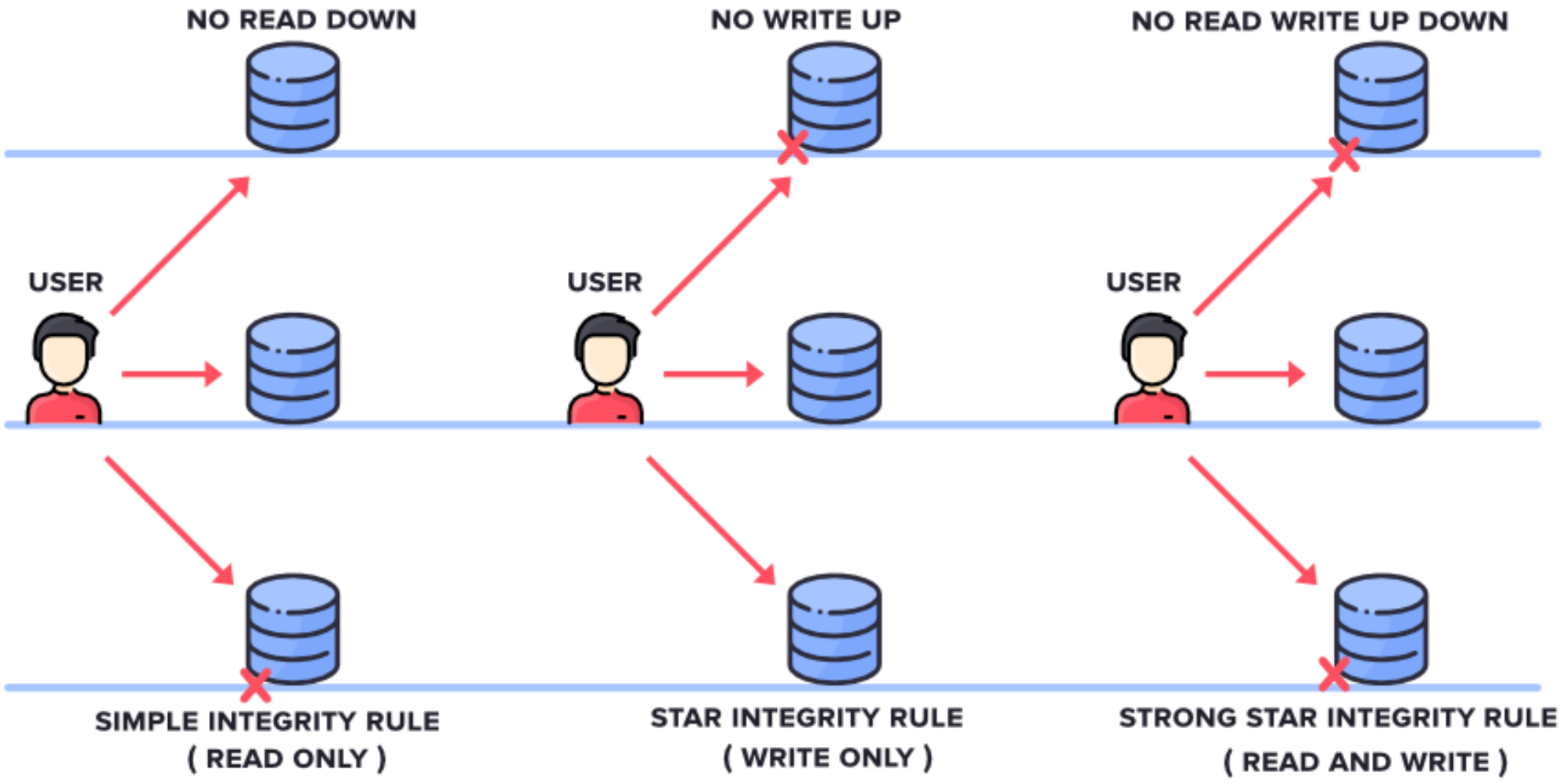
BELL - LAPADULA MODEL



Biba

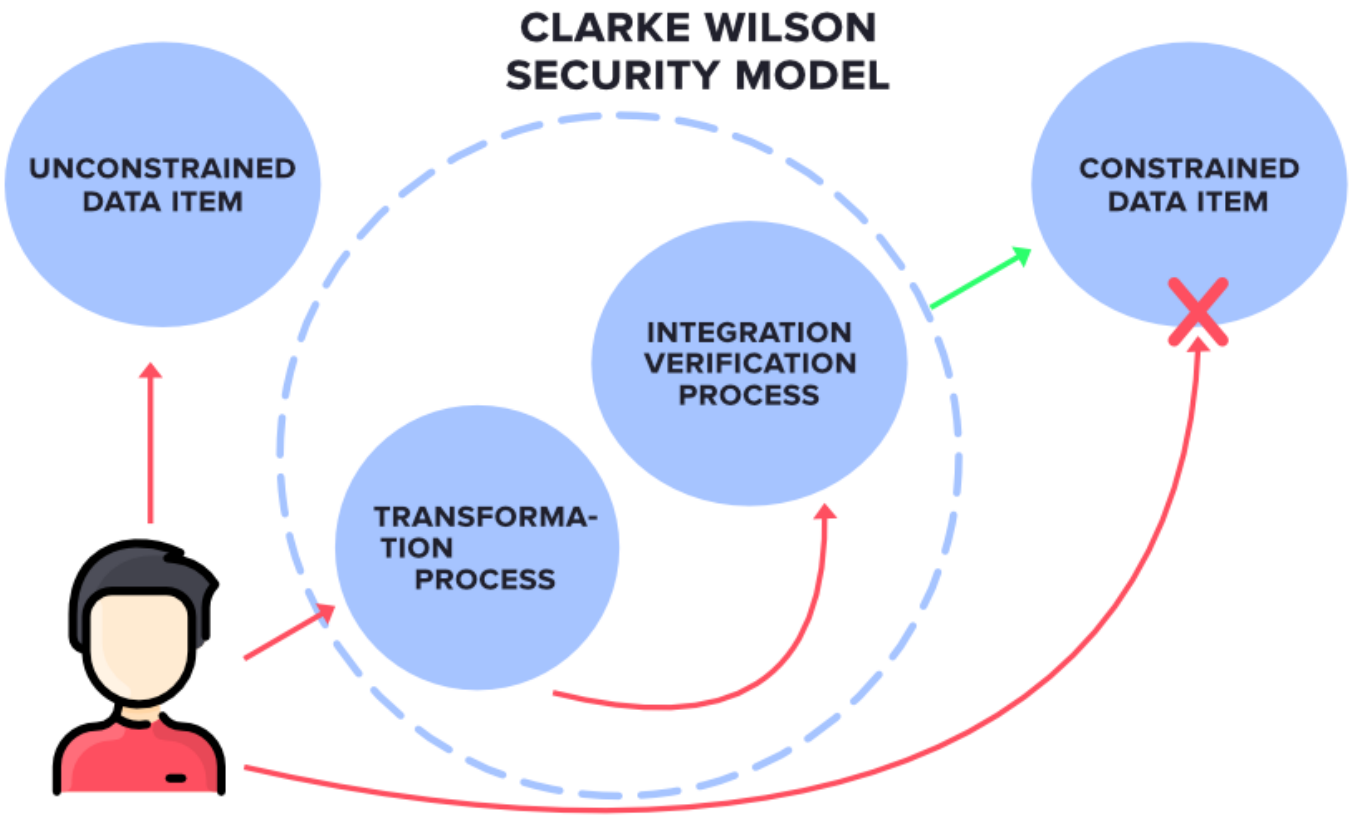
- The *Biba model* was the first model developed to address the concerns of integrity. Originally published in 1977, this lattice-based model has the following defining properties:
  - **Simple integrity property**—This property states that a subject at one level of integrity is not permitted to read an object of lower integrity.
  - **Star * integrity property**—This property states that an object at one level of integrity is not permitted to write to an object of higher integrity.
  - **Invocation property**—This property prohibits a subject at one level of integrity from invoking a subject at a higher level of integrity.
- Biba addresses only the first goal of integrity—protecting the system for access by unauthorized users.
- Availability and confidentiality are not examined. It also assumes that internal threats are being protected by good coding practices, and therefore focuses on external threats.

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)

Clarke Wilson Security Model

- The Clark-Wilson model was created in 1987.
- It differs from previous models because it was developed with the intention to be used for commercial activities.
- This model addresses all the goals of integrity.
- Clark Wilson dictates that the separation of duties must be enforced, subjects must access data through an application, and auditing is required. Some terms associated with Clark Wilson include
  - User
  - Transformation procedure
  - Unconstrained data item
  - Constrained data item
  - Integrity verification procedure
- Clark-Wilson features an access control triple. The access control triple is composed of the user, transformational procedure, and the constrained data item.
- It was designed to protect integrity and prevent fraud. Authorized users cannot change data in an inappropriate way. It also differs from the Biba model in that subjects are restricted.
- This means a subject at one level of access can read one set of data, whereas a subject at another level of access has access to a different set of data.



- SUBJECT: It is any user who is requesting for Data Items.
- CONSTRAINED DATA ITEMS: It cannot be accessed directly by the Subject. These need to be accessed via Clarke Wilson Security Model
- UNCONSTRAINED DATA ITEMS: It can be accessed directly by the Subject.
- The Components of Clarke Wilson Security Model
    - TRANSFORMATION PROCESS: 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
    - INTEGRATION VERIFICATION PROCESS: The Integration Verification Process will perform Authentication and Authorization. If that is successful, then the Subject is given access to Constrained Data Items.

- Clark-Wilson controls the way in which subjects access objects so that the internal consistency of the system can be ensured and that data can be manipulated only in ways that protect consistency.
- Integrity verification procedures (IVPs) ensure that a data item is in a valid state. Data cannot be tampered with while being changed and the integrity of the data must be consistent.
- Clark-Wilson requires that all changes must be logged.
- Clark-Wilson is made up of transformation procedures (TP).
- Constrained data items (CDI) are data for which integrity must be preserved. Items not covered under the model are considered unconstrained data items (UDIs).
- The Clark Wilson model requires that users be authorized to access and modify data, and that it deals with three key terms: tampered, logged, and consistent, or “TLC.”

Take-Grant Model

- The *Take-Grant* model is another confidentiality-based model that supports four basic operations: take, grant, create, and revoke.
- This model allows subjects with the take right to remove take rights from other subjects.
- Subjects possessing the grant right can grant this right to other subjects.
- The create and revoke operations work in the same manner: Someone with the create right can give the create right to others and those with the revoke right can remove that right from others.

Brewer and Nash Model

- The *Brewer and Nash* model is similar to the Bell-LaPadula model and is also called the *Chinese Wall model*. It was developed to prevent conflict of interest (COI) problems.
- 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 is more context-oriented in that it prevents a worker consulting for one firm from accessing data belonging to another, thereby preventing any COI.

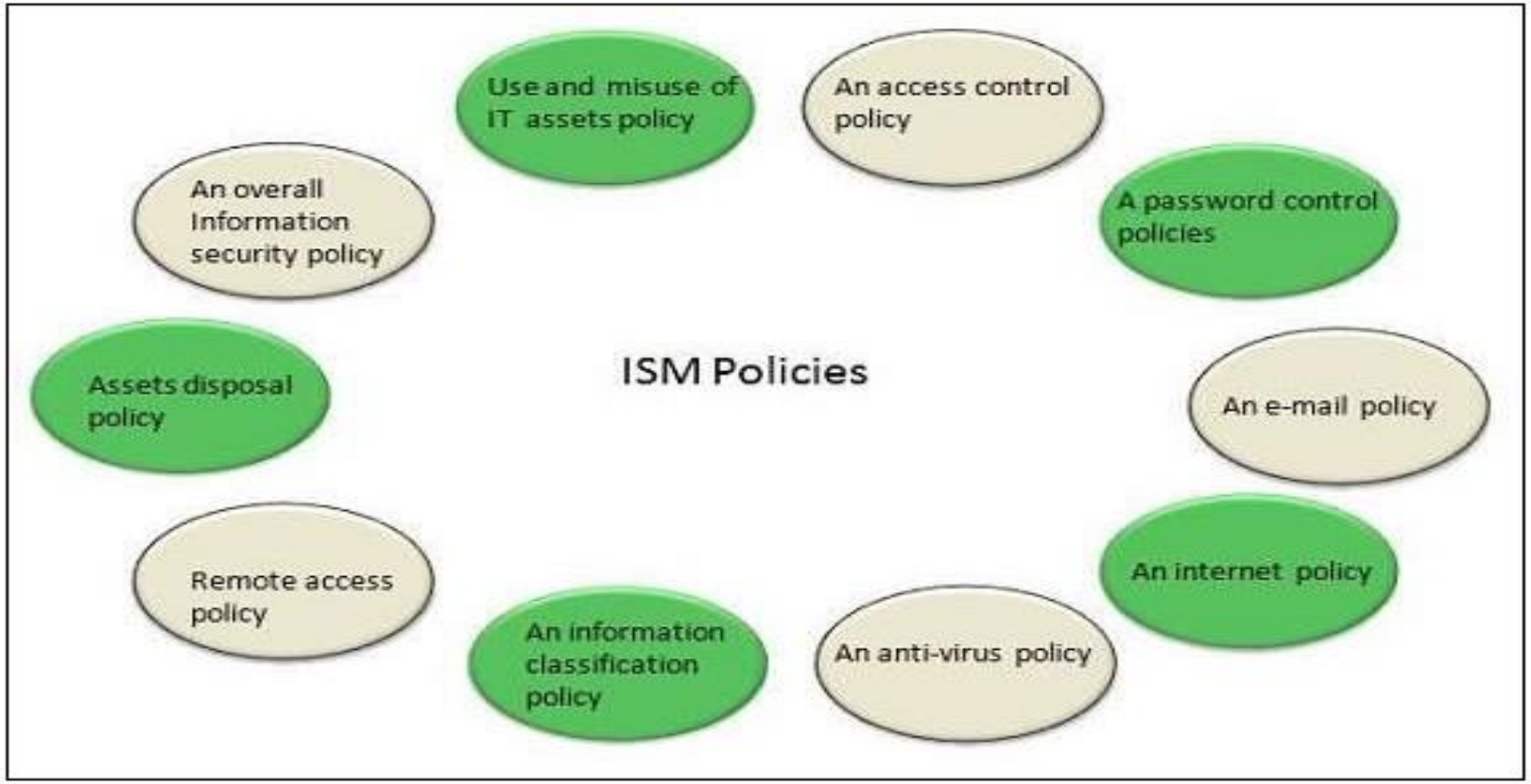
- **Information Security Management (ISM)**

Information Security Management (ISM)

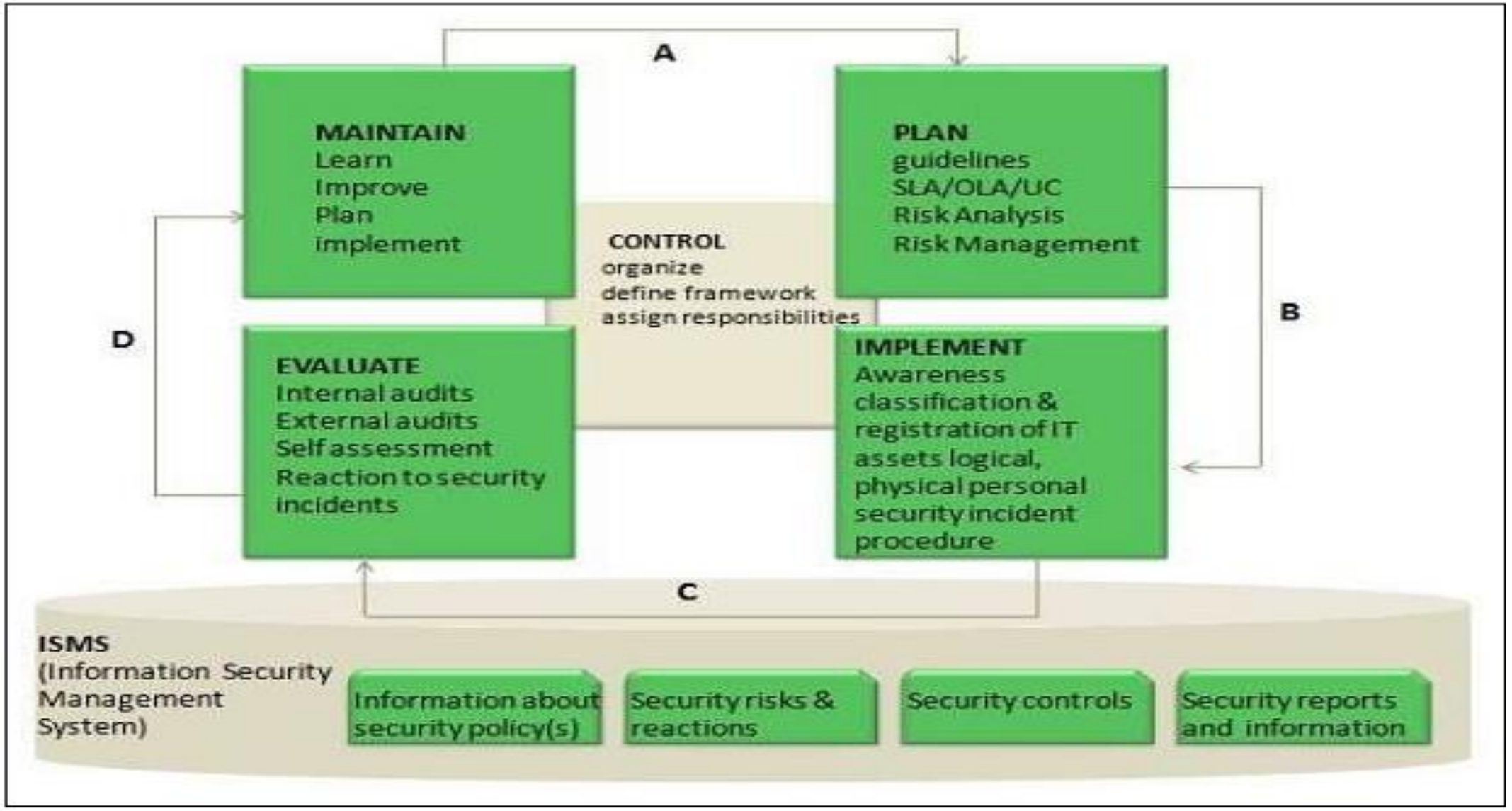
- Ensures confidentiality, authenticity, non-repudiation, integrity and availability of organization data and IT services.
- It also ensures reasonable use of organization's information resources and appropriate management of information security risks.
- Information security is considered to be met when:
  - Information is observed or disclosed only to authorized persons
  - Information is complete, accurate and protected against unauthorized access (integrity)
  - Information is available and usable when required and the systems providing the information resist attack and recover from or prevent failures (availability)
  - Business transaction as well information exchanges between enterprises, or with partners, can be trusted (authenticity and non-repudiation)

ISM Security Policy

- It cover all areas of security, be appropriate, meet the needs of business and should include the policies shown in the following diagram:



ISM Framework



Key elements in ISM Framework

- ISM framework involves the following key elements –

a) Control

- The objective of Control element is to:
  - Establish an organization structure to prepare, approve and implement the information security policy
  - Allocate responsibilities
  - Establish and control documentation

b) Plan

- The purpose of this element is to devise and recommend the appropriate security measures, based on an understanding of the requirements of the organization.

c) Implement

- This key element ensures that appropriate procedures, tools and controls are in place to underpin the security policy.

d) **Evaluation**

- The objective of Evaluation element is to:
  - Carry out regular audits of the technical security of IT systems
  - Supervise and check compliance with security policy and security requirements in SLAs (Service Level Agreements) and OLAs (operational level agreement)

e) Maintain

- The objective of Maintain element is to:
  - Improve on security agreements as specified in, for example, SLAs and OLAs
  - Improve the implementation of security measures and controls

Other key measures

- **Preventive**
  - This key element ensures prevention from security incidents to occur. Measures such as control of access rights, authorization, identification, and authentication and access control are required for this preventive security measures to be effective.
- **Reductive**
  - It deals with minimizing any possible damage that may occur.
- **Detective**
  - It is important to detect any security incident as soon as possible.
- **Repressive**
  - This measure is used to counter any repetition of security incident.
- **Corrective**
  - This measure ensures damage is repaired as far as possible.

- Thank you