Chapter 2
Information security architecture and Model

(24 Marks)
Information security and Risk Management, Security policies, guidelines, standards
Trusted computing base, Rings of Trust, Protection Mechanisms in a trusted Computing Base
System security assurance concepts, Trusted computer security Evaluation Criteria
Information Technology security Evaluation Criteria, Confidentiality and Integrity Models.

Information Security and Risk Management

- **RISK = ASSETS x THREATS x VULNERABILITIES**
- **Assets:** Hardware, Software, Data and Documentation, Personnel, procedures, models etc.
- Threats: Actions taken by attackers
- Vulnerabilities: Weaknesses in the system

Risk Management

Components of Risk Management

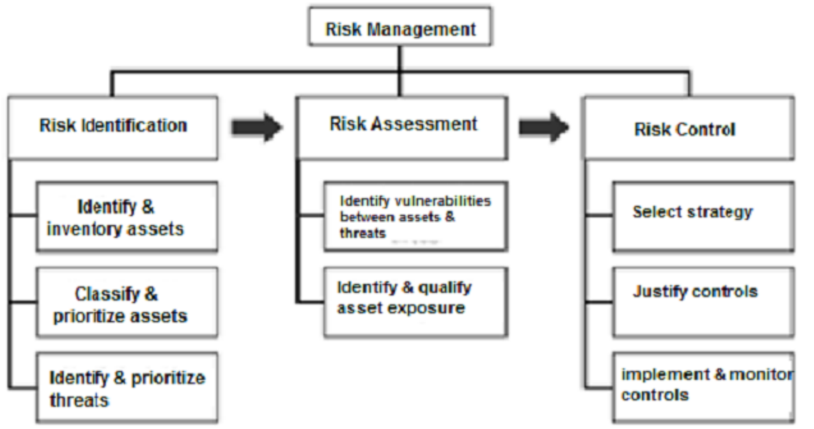

Risk Management
Risk Identification
Identify & inventory assets
Classify & prioritize assets
Identify & prioritize threats
Risk Assessment
Identify vulnerabilities between assets & threats
Identify & qualify asset exposure
Risk Control
Select strategy
Justify controls
implement & monitor controls

Fig: Components of Risk Management

Risk management: process of identifying and controlling risks facing an organization

- Risk identification: process of examining an organization’s current information technology security situation.
- Risk Assessment: Risk assessment is the determination of the extent to which the organization‘s information assets are exposed or at risk
- Risk control: applying controls to reduce risks to an organizations data and information systems

Risk Control Strategies

- Once ranked vulnerability risk worksheet complete, must choose one of four strategies to control each risk:

1. Avoidance: Apply safeguards that eliminate or reduce residual risk
2. Transference: Transfer the risk to other assets, other processes or other organizations.
3. Mitigation: Reduce the impact should the vulnerability be exploited
4. Acceptance: Understand the consequences and accept the risk without control or mitigation

RISK ANALYSIS (RA)

Risk can be calculated by Risk Analysis (RA) and it is the identification and estimation of risks.

1. Quantitative Risk Analysis

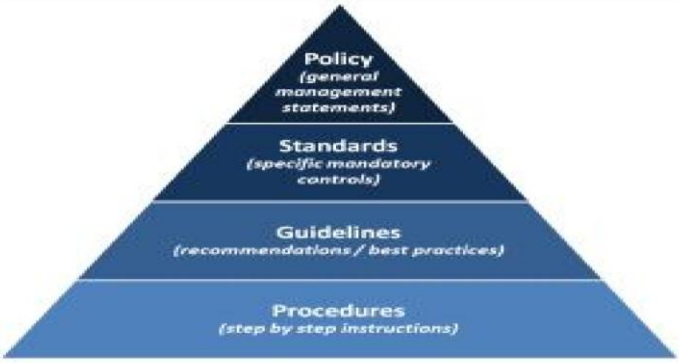
- A process for assigning a numeric value to the probability of loss based on known risks, on financial values of the assets and on probability of threats
- It is used to determine potential direct and indirect costs to the company based on values assigned to company assets and their exposure to risk eg the cost of replacing as asset, the cost of lost productivity or the cost of diminished brand reputation

2. Qualitative Risk Analysis

- It is a collaborative process of assigning relative values to assets, assessing their risk exposure, and estimating the cost of controlling the risk. It differs from quantitative risk analysis in that it utilizes relative measures and approximate costs rather than precise valuation and cost determination. In qualitative risk analysis:

1. Assets can be rated based on criticality - very important, important, not-important etc.
2. Vulnerabilities can be rated based on how it is fixed - fixed soon, should be fixed, fix if suitable etc.
3. Threats can be rated based on scale of likely - likely, unlikely, very likely etc.

Security Policies, Standards, Guidelines and Procedures


Policy
(general management statements)
Standards
(specific mandatory controls)
Guidelines
(recommendations / best practices)
Procedures
(step by step instructions)

An information security policy consists of **high level statements** relating to the protection of information across the business and should be produced by senior management.

- The policy outlines security roles and responsibilities, defines the scope of information to be protected, and provides a high level description of the controls that must be in place to protect information.
- Policies are of following types:
  - Senior Management Policy
  - Regulatory Policy
  - Advisory Policy
  - Informative Policy

Q: Explain different information security policies and guidelines. (W-14)

Ans: Different Information Securities Policies:-

1. Senior Management Statement of Policy:
   - This is the first step in the policy creation process. This is a general, high level statement of policy that contains the following elements:
   - An acknowledgement of the importance of computing and networking resources, that are part of the information system, to the organization‘s business model;
   - A statement of support for Information security throughout the business enterprises;
   - A commitment to authorize and manage the definition of the lower level standards, procedures and guidelines.
2. Regulatory Policy:

   These are security policies that an organization must implement owing to compliance, regulation or other legal requirements as prevalent in the organization‘s operating environment, both internal and external.

3. Advisory Policy:

   - These are security policies that may not be mandated but are strongly recommended.
   - Normally, the consequences of not following them are defined.

- An organization with such policies wants its employees to consider these polices mandatory.

4. Informative Policy:

- These are policies that exist simply to inform the reader.
- There are no implied or specified requirements, and the audience for this information could be certain internal entities or external parties.

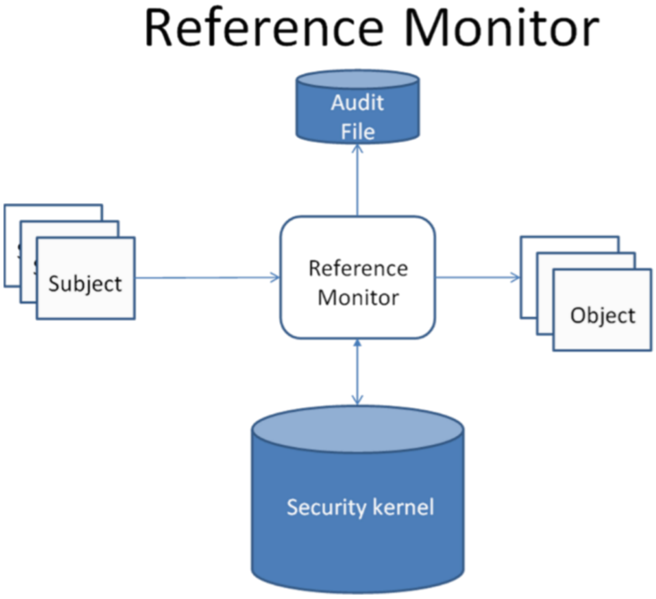
Standards

- Standards consist of specific **low level mandatory controls** that help enforce and support the information security policy.
- Standards help to ensure security consistency across the business and usually contain security controls relating to the implementation of specific technology, hardware or software.
- For eg a password standard may set out rules for password complexity and a Windows standard may set out the rules for hardening Windows Clients.
- **Guidelines**
- Guidelines consist of **recommended, non-mandatory controls** that help support standards or serve as a reference when no applicable standard is in place.
- Guidelines should be viewed as best practices that are not usually requirements, but are strongly recommended.
- For example, a standard may require passwords to be 8 characters or more and a supporting guideline may state that it is best practice to also ensure the password expires after 30 days
- **Procedures**
- Procedures consist of **step by step instructions** to assist workers in implementing the various policies, standards and guidelines.
- Whilst the policies, standards and guidelines consist of the controls that should be in place, a procedure gets down to specifics, explaining how to implement these controls in a step by step fashion.
- For example, a procedure could be written to explain how to install Windows securely, detailing each step that needs to be taken to harden/secure the operating system so that it satisfies the applicable policy, standards and guidelines.

Trusted Computing Base

- Trusted Computing Base is a complete protection mechanism in any computer system and it is responsible for enforcing system-wide information security policies.

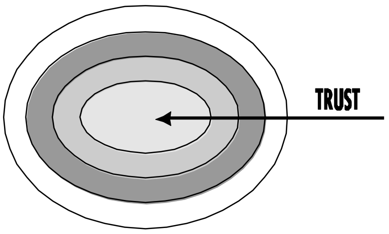
- It is a combination of hardware, software and firmware that work together to implement a combined security policy for system or a product.
- Software model/abstract machine is a reference monitor that passes all access from any subject (user) to any object (data/file) but it cannot be avoided. It gives access to objects by subjects. The reference monitor has three properties :
  - Cannot be bypassed and controls all access.
  - Cannot be altered and is protected from modification or change
  - Can be verified and tested to be correct.
- It stands between each subject and object and its role is to verify the subject, meets the minimum requirements for access to an object.



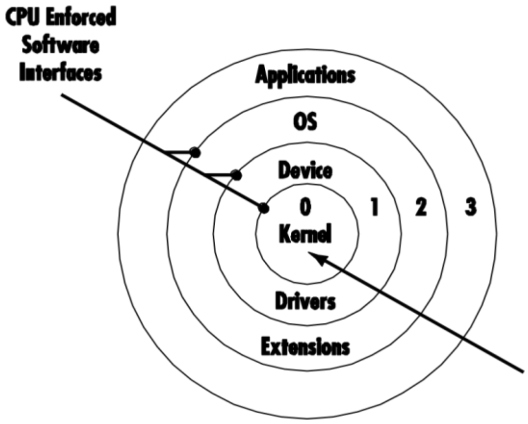
- In Unix/Linux OS, a security kernel acts as a reference monitor. The security kernel handles all user /application requests for access to system resources.
- The reference monitor operates at the security perimeter- the boundary between the trusted and untrusted area.
- Components outside the security perimeter are not trusted.
- According to TCB, a trusted system is a system that should meet user's requirement of security, effectiveness and reliability.

Rings of Trust

- Trust in a system moves from the outside to the inside in a unidirectional mode

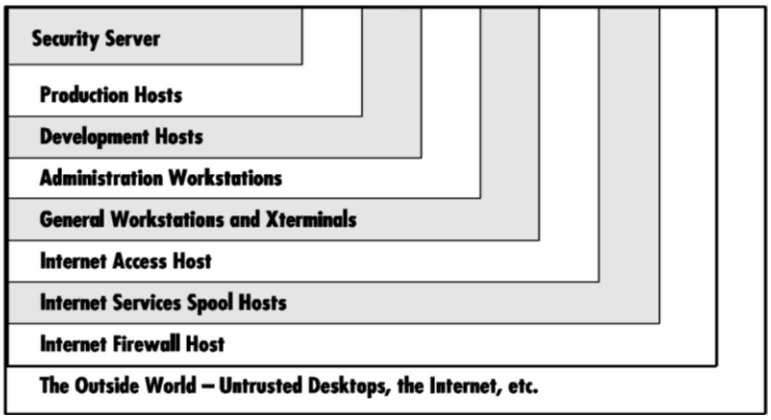


- Rings of trust in stand-alone systems



The protection ring model provides the OS with various levels at which to execute code or to restrict that code's access.

- Layer 0: the most trusted level. The OS kernel resides at this level . Any process running at layer 0 is said to be operating in privileged mode.
- Layer 1: contains non-privileged portions of the OS.
- Layer 2: where I/O drivers, low level operations and utilities reside,
- Layer 3: where applications and processes operate. This is the level at which individuals usually interact with the OS.
- Protection rings are part of the trusted computing base concept.


Security Server
Production Hosts
Development Hosts
Administration Workstations
General Workstations and Xterminals
Internet Access Host
Internet Services Spool Hosts
Internet Firewall Host
The Outside World – Untrusted Desktops, the Internet, etc.

Firstly, the hosts of networks are divided into rings depend on the security rating of services provided by hosts to network. Then created ring can be used as a basic for trust between hosts of the network.

The hierarchy of the ring can be decided based on

■ Is the host in a physically secured computer room?

■ Does the host have normal (as opposed to privileged) user accounts?

■ Is this host at a remote site and hence less trustworthy than the ones in the central computer room?

■ Does this host operate software that relies on data obtained from the Internet?

■ Does this host provide mission-critical services? How many people in the company would be affected by downtime on this host?

The following general rules apply to constructing rings of trust in networked systems:

■ Each host trusts those hosts in a more inner ring than itself.

■ No host trusts any host in a more outer ring than itself.

■ Each host may trust those hosts in the same ring as itself. where a ring has been segmented into separate subnetworks, a host in one segment does not trust hosts in other segments.

Protection Mechanisms in a Trusted Computing Base

1. Process isolation

   Every process has its own address space for storing data and code of application. Because if process isolation it is possible to prevent processes from accessing other process's data.
   This will prevent data leakage and modification in the memory

2. Principle of least privilege

   Every process has least privilege which is required to access resources to perform its function. This will prevent data from being exploited.

3. Hardware segmentation
   It relates to the segmentation of memory into protected segments
   It prevents user processes from being able to access both another process's allocated memory and system memory.
4. Layering
   A process operation is divided into number of layers to perform various function
   Each layer deals with particular type of action.
5. Abstraction: It is a process of defining a specific set of permissible values as well as operations for an object. This will help in maintain security by ignoring implementation details.

6. Data hiding (also known as information hiding)

It is process of assuring that information available at one processing level is not available in another, regardless of whether it is higher or lower

7. Information storage

It is a process of retaining a physical state of information for specific interval of time, possibly even after electrical power to the computer is removed. Following are the types of information storage: Primary Memory (RAM), secondary memory (Hard Disk) , sequential memory etc.

8. Closed System vs. Open System

Closed systems are of a proprietary nature. They use specific operating systems and hardware to perform the task and generally lack standard interfaces to allow connection to other systems

An open system uses standard interface that allows connections between different systems. This system gives full access to users.

9. Multitasking

Multitasking is a capability of running multiple tasks at a time in synchronized way

10. Multiprogramming

Multiprogramming allows execution of multiple programs.

11. Multiprocessing

Multiprocessing allows simultaneous execution of two or more programs by more than one processor (CPU)

12. Finite-state machine

It is a device which stores state of process at a given time. The operation of finite state machine is based on the input given to the device. According to the input given, it will change the output or the state that is already stored. The new state is depending upon the old state and input.

System Security Assurance Concepts

- IT Security System has two types of requirements:

  1) Functional requirements

     - ❑ Describe what a system should do

  2) Assurance requirements

     - ❑ Describe how functional requirements should be implemented and tested

Goals of Security Testing

❑ It verifies that the functions designed to meet a security requirement operate as expected .

❑ In addition, it validates that the implementation of the function is not flawed or random

Formal Security Testing Models

1. Trusted Computer System Evaluation Criteria (TCSEC)
   United States in the early 1980s
2. Information Technology Security Evaluation Criteria (ITSEC)
   Europe in 1991 by the European Commission
3. Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)
   Canada in early 1993
4. Federal Criteria for Information Technology Security (FC)
   United States in early 1993
5. Common Criteria Today's standard

1. Trusted Computer System Evaluation Criteria (TCSEC)

- Trusted Computer System Evaluation Criteria (TCSEC) is a 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.
- This evaluation criterion is published in a book with an orange cover, which is called appropriately the Orange Book
- The TCSEC was used to evaluate, classify and select computer systems being considered for the processing, storage and retrieval of sensitive or classified information.
- TCSEC provides a graded classification of systems that is divided into hierarchical divisions of security levels:
- The TCSEC defines four divisions:
  A. Verified protection
  B. Mandatory protection
  C. Discretionary protection
  D. Minimal security.
- The classification A represents the highest level of security and D represents the lowest level of security.
- Each division can have one or more numbered classes and each has a corresponding set of requirements that must be met for a system to achieve that particular rating.

D — Minimal protection

Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division

C — Discretionary protection

o C1 — Discretionary Security Protection

o C2 — Controlled Access Protection

B — Mandatory protection

o B1 — Labeled Security Protection

o B2 — Structured Protection

o B3 — Security Domains

A — Verified protection

o A1 — Verified Design

- The classes with higher numbers indicate a greater degree of trust and assurance. So B2would offer more trust than B1, and C2 would offer more trust than C1.
- The criteria include four main topics: **security policy, accountability, assurance, and documentation**, but these actually break down into **seven different areas**:

1. **Security policy** the policy must be explicit and well defined and enforced by the mechanisms within the system.
2. **Identification** Individual subjects must be uniquely identified.
3. **Labels** Access control labels must be associated properly with objects.
4. **Documentation** this includes the test, design, specification documents, user guides, and manuals.
5. **Accountability** Audit data must be captured and protected to enforce accountability.
6. **Life cycle assurance** Software, hardware, and firmware must be able to be tested individually to ensure that each enforces the security policy in an effective manner throughout their lifetimes.
7. **Continuous protection:** The security mechanisms and the system as a whole must perform predictably and acceptably in different situations continuously.

- These categories are evaluated independently, but the rating that is assigned at the end does not specify these different objectives individually. The rating is a sum total of these items.
- Each division and class incorporates the requirements of the ones below it.
- This means that C2 must meet its criteria requirements and all of C1 requirements, and B3 has its requirements to fulfill along with those of C1, C2, B1, and B2.
- Each division or class ups the ante on security requirements and is expected to fulfill the requirements of all the classes and divisions below it.

2. Information Technology Security Evaluation Criteria (ITSEC)

- ITSEC is developed by European country for security equation criteria.
- ITSEC focuses more on integrity and availability. It tries to provide a uniform approach to product and system.
- It also introduces the **security target** (ST), a written document that contains
  - Policy for system security.
  - Required mechanism for security.
  - Required rating to claim for minimum strength.
  - Level for evaluating targets –functional as well as evaluation.(F-xx and E-yy).
- ITSEC classes contain hierarchical structure where every class will be added to the class above it. This class contains some particular function.
  - F-IN This class will provide high integrity.
  - F-AV This class will provide high availability.
  - F-DI This class will provide high data integrity.
  - F-DX This class is used for networks. Of provide high integrity while exchanging data in networking.
- ITSEC uses following classes from E0 to E6 to evaluate the security.
- E0 – Minimal protection.
- E1 – Security target and informal architecture design must be produced.
- E2 – An informal detail design and test document must be produced.

- E3 – Source code or hardware drawing to be produced. Correspondence must be shown between source codes of detailed design.
- E4 – Formal model of Security and Semi – formal specification of Security function architecture and detailed design to be produced.
- E5 – Architecture design explain the inter relationship between security component.
- E6 – Formal description of architecture and Security function to be produced. Security models are mathematical representations of abstract machines that describe how a reference monitor is designed to operate

- Commonly used models:
  1. Bell-LaPadula model [Confidentiality Model]
  2. Biba integrity model [Integrity Model]
  3. Clark and Wilson Model
  4. Noninterference Model
  5. State machine model
  6. Access matrix model
  7. Information flow model

Bell-LaPadula model (BLP) : Confidentiality Models

- ❑ This model was developed in the 1970s for the US Military by David Bell and Leonard LaPadula of Mitre Corporation
- ❑ is a ***confidentiality model*** intended to preserve the principle of least privilege
- ❑ It was developed in response to a single problem –information leakage. E.g The Military using time-sharing mainframe systems.
- ❑ This model can specify how security tools are used to achieve the desired level of confidentiality.
- ❑ BLP model defines the relationship between objects (files) and subjects (users)
- ❑ BLP is a formal model of security policy which defines set of rules for access controls like:
- ❑ **Dominance Relation:**

  Users with a particular clearance will only be able to access files of a particular classification and below.

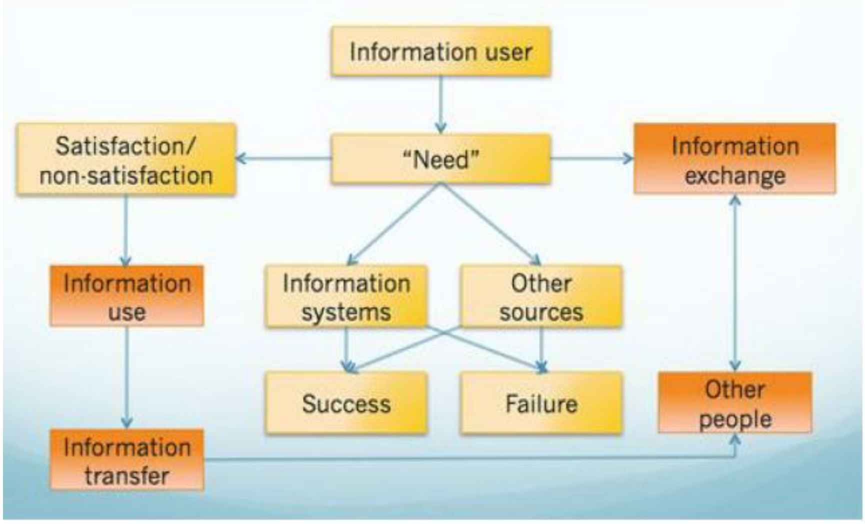
- ❑ **Discretionary Security:** specific subjects(users) are granted specific modes of access.
  - ❑ **Data flows upwards**: BLP enforces the confidentiality aspect of access control in that data can only move up from lower levels of classification to higher
  - ❑ BLP is also categorized as an Information Flow Model

- ❑ BLP was the first model to define 3 fundamental modes of access- read, write and read/write, though users cannot be assigned to more than one access mode.
- ❑ BLP has three properties:
  - ❑ **Simple Security Property**: Users can read data of a lower classification
  - ❑ **Star Security Property**: Users can write data to an area of higher classification
  - ❑ **Strong Star (Tranquility) Property**: Users can read and write to own level only.
- ❑ BLP is a WURD (Write Up, Read Down)

Biba integrity model

- ■ Integrity is the protection of system data from intentional or accidental unauthorized changes
- ■ Biba Uses a ***read up*****,** ***write down [RUWD]*** approach. Subjects cannot read objects of lesser integrity and subjects cannot write to objects of higher integrity
- ■ The major drawback of BLP Model is that users were free to read all data at their own and lower levels of classification.
- ■ Hence Ken Biba developed a model that considered data integrity
- ■ Biba model is concerned with preventing data from low integrity environments polluting high integrity data.
- ■ The challenge of the security program is to ensure that data is maintained in the state that users expect.
- ■ The security program cannot improve the accuracy of data that is put into the system by users, it can help ensure that any changes are intended and correctly applied.
- ■ Biba Model has following three properties:
- ■ **Simple Integrity Property** : Data can be read from a higher integrity level.
- ■ **Star Integrity Property**: Data can be written to a lower integrity level.
- ■ **Invocation Property:** User cannot request service(invoke) from a higher integrity level.
- ■ In Biba model, the subject with top secret clearance can able to see information that is labelled with top secrets clearance.
- ■ Higher clearances will not view information at the lower level of integrity as well as highest level of integrity

- **Clark and Wilson model**
- This model was published in year 1987 by David Clark and David Wilson builds on BLP and Biba.
- The Clark-Wilson security model is based on preserving information integrity against the malicious attempt of tampering data.
  - It addresses all three integrity goals:
  - Preventing unauthorized users from making any modifications
  - Preventing authorized users from making unauthorized modifications
  - Maintaining internal and external consistency.
- The Clark-Wilson model requires well-formed transaction.
- A well-formed transition is that operations and data feeds and processing are consistent within the system



  - ❑ A well-formed transaction is one that only permits modification of data if that modification meets the three integrity goals listed above.
  - ❑ Data objects can only be manipulated by a certain set of programs. Users have access to the programs rather than to the data. (e. g. this is like the WWW or a database).

Separation of duties: assigning different roles to different users. Users might have to collaborate in order to achieve some secure operation.

- ❑ The Clark-Wilson model also tries to address the relationship between the system and the acceptance of information from outside world by insisting on auditing of transactions.
- ❑ This will not help security/integrity but it can detect breaches.

In summary:

- ❑ Subjects/users are identified and authenticated.
- ❑ Objects/data can only be accessed by authorized programs (ensures integrity).
- ❑ Subjects/users only have access to certain programs.
- ❑ An audit log is maintained over external transactions.
- ❑ The system must be certified in order for it to work.

- **Noninterference model**
- covers ways to prevent subjects operating in one domain from affecting each other in violation of security policy
- **State machine model**
- is an abstract mathematical model consisting of state variables and transition functions
- **Access matrix model**
- is a state machine model for a discretionary access control environment

- **Information flow model**
- It simplifies analysis of covert channels used to communicate between two cooperating processes at different security levels to exchange information in such a way that it violated the security policy of the system.

MSBTE Questions

Summer 2016

- Explain TCB (Trusted Computing Base) with respect to Information Security
- How to evaluate information security? Write down any two criterias to evaluate information security.
- Define term integrity. Explain integrity model with example.
- Describe following with respect to information security.
  - Risk Management
  - Security and Policies
  - Standards and guidelines
- Explain the concepts of system security assurance.
- Describe confidentiality model of information security**.**

Winter 2015

- What is Risk? Describe Risk Management.
- State the common criteria for information security evaluation.
- State the security guidelines of information security.
- Describe the term rings of trust.
- Explain the protection mechanisms in a trusted computing base.
- Explain the concept of TCB.
- Describe BIBA model of integrity.
- Describe ITSEC with its classes

Summer 2015

- With respect to information security define following term:
    1) Trust computing base (2M)
    2) Standard (1 M)
    3) Security policy (1 M)
- Define risk. Describe how risk is managed for information security.(Definition of Risk-2M, Risk Management-4M)
- Describe ring of trust for single system and for networking.(Single System 2 Marks; Networking 2 Marks).
- Describe any four type of protection mechanism in TCB.(1 Mark for each type of protection).
- Describe then term TCSEC. (Description 4 Marks)
- Describe Clark Wilson model of integrity.(diagram -1M Explanation 3 Marks)

Winter 2014

- State the meaning of information security and risk management with example. (Meaning of Information Security - 1 Mark, Meaning of risk management - 1 Mark, Example -1 Mark each).
- Explain different information security policies and guidelines. (Security Policies - 4 Marks (one policy -1 Mark), Guidelines - 2 Marks).
- Mention and explain integrity model. (Description - 2 Marks; Rules - 2 Marks).
- Describe BIBA model of security.(For Explanation- 4 Marks).
- Describe ITSEC with its classes. (For Explanation- 4 Marks)
- Describe TCSEC. (Any relevant description shall be consider; Description - 1 Mark, Policy - 1 Mark, Accountability - 1 Mark, Classes - 1 Mark).