4

SECURITY FOR E-GOVERNMENT

CHAPTER OUTLINE

After comprehensive study of this chapter, you will be able to:

- Challenges and Approach of E-government Security
- Security Management Model
- E-Government Security Architecture
- Security Standards

INTRODUCTION

E-Governance involves Information Technology enabled initiatives that are used for improving the interaction between Government and citizens or Government and business as well as the internal Government operations.

To provide "trusted" services, e-Governance needs to focus on Effectiveness, Efficiency, and Flexibility & Transparency. If the citizen or end user is to derive maximum benefit from the provision of e-Services through e- Governance, the e-Service must possess the following attributes:

- The users must know the information about the available e-services
- The users must be aware of the benefits of these services
- The user should be able to locate the e-services easily
- The e-services must be accessible to all members of the intended target groups
- The information from the e-services should be comprehensive, correct, readily available, and easy to understand with respect to language and structure
- The provision of e-services should be confidential, and in no way violate the privacy of either party
- The design of e-Governance applications should comply with the existing legal data protection requirements and relevant legal and statutory laws & acts.
- From the attributes it becomes evident that the "value" of information held and processed by the e-Governance service needs to be protected at all levels (i.e. Application, Infrastructure, and Operation & Management). Information security is intended to safeguard the information assets and is determined in terms of confidentiality, integrity and availability.

- **Confidentiality**: Protecting sensitive information from unauthorized disclosure or intelligible interception
- **Integrity:** Safeguarding the accuracy and completeness of information and software; protecting data from unauthorized, unanticipated or unintentional modification
- **Availability:** Ensuring that information and vital IT services are available when required To safeguard the "value" of information, effective security measures (that can limit the risks and vulnerability) need to be implemented harmoniously. These security measures provide layers of protection to the Application, It infrastructure, Control and Management in a e governance computing environment.

In context of Security, services provided by e-government program are categorized with respect to functional processes as :

(a) **Publishing:** Publishing involves simply posting information on a publicly accessible Web site.

(b) **Interactive processing:** E-government interactive processing involves private citizens or other user entities reading instructions published on agency Web sites and following those instructions to submit reports, applications, or other service requests (e.g., submit tax returns, apply for licenses or other services, renew licenses)

(c) **Transaction processing:** Transaction processing includes processing of information submitted via interactive e-government Web sites, providing notification of approval for actions to be taken on the basis of that information, and activation of implementation processes (e.g., billing, payment, licensing, permit issuance, contract awards, invoice approvals, etc.).

(d) **Service delivery:** Service delivery goes beyond the transaction approval component to transaction processing, including the actual execution of actions approved on the basis of e-government interactions. Examples of such actions include acceptance of credit card payments or electronic funds transfers, execution of government payments (e.g., benefits, grants, refunds, or payments for services or products) by electronic fund transfers, and delivery of licenses or permits.

CHALLENGES AND APPROACH OF E-GOVERNMENT SECURITY

Challenges and Approach of E-Government Security

Threats to the security of information in an e-government environment can include natural and accidental events (e.g., flooding, fire, storms, human error, and environmental problems) and deliberate threats (e.g., sabotage, fraud, information theft, Trojan horses, hacking, viruses, logic bombs). Deliberate attacks may come from criminals, hackers, terrorists, disenchanted employees, curious or mischievous users, journalists, state-sponsored or industrial spies, or state-sponsored or industrial saboteurs. Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for security. We will discuss each one of them and security challenges related to them in context of E governance.

1. **Availability**

Availability is defined as "ensuring timely and reliable access to and use of information." Availability concerns affect publishing, interactive processing, transaction processing, and service delivery e-government activities. Availability concerns include those resulting from system faults, those intrinsic to the technologies employed to provide e-government services, and malicious activities intended to prevent access to or use of information (denial of service attacks). Although fault-related availability and intrinsic availability concerns are not usually treated as security issues, they can significantly affect access to and use of e-government services, and countermeasures that are employed against denial of service and integrity threats can often mitigate system fault and intrinsic availability concerns.

(a) **Fault-related availability concerns:** System faults that can affect availability of services include hardware faults, changes in program or data structures due to transients or design errors, and failures in other system facilities that are not computer based.

(b) **Intrinsic availability concerns:** Intrinsic availability concerns include obsolescence of storage and recovery mechanisms, deterioration of magnetic media, ephemeral continuity of access channels such as addresses and protocols, and loss of facilities due to physical damage or support infrastructure problems.

(c) **Denial of service concerns:** Government sites are attractive targets for malicious activities intended to prevent access to, or use of, information (denial of service attacks). These can range from relatively unsophisticated assaults that result in temporary degradation of service response times to crippling attacks that corrupt or destroy system resources. Denial of service attacks can be launched from a variety of sources and can take a number of forms.

(d) **Individual or informally organized hackers:** Most denial of service attacks against e-government services have been launched by individuals or informally organized groups of hackers. Some of these have resulted in significant disruption and expense to the taxpayer.

2. **Integrity**

Integrity is defined as "guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity." Integrity concerns affect publishing, interactive processing, transaction processing, and service delivery of e-government activities. If published information, requests for information received from users, or authorizations or payments issued to users are improperly modified or destroyed, routed, or ascribed, then damage to confidence in the government, to user or customers, or to government assets can result.

(a) **Data Content Integrity Issues**

Data content integrity issues are associated with unauthorized modification or destruction of e-government information content. This can involve modification or destruction of

- information electronically published by the government;
- information associated with reports, applications, or other service requests provided by private citizens or other user entities (e.g., submit tax returns, apply for licenses or other services, renew licenses, order products or services, or provide notification of address change or other status changes);
- notification to private citizens or other user entities of approval actions or activation of implementation processes (e.g., billing, payment, licensing, permit issuance, contract awards, invoice approvals, etc.); and
- information executing actions approved on the basis of e-government interactions (e.g., credit card payment information or electronic funds transfer information, electronic fund transfer information, and licenses or permits).

(b) **Intentional modification of data:** Data may be modified or destroyed within e-government processors (e.g., Web servers) or in transit. In the case of the former, an attacker must gain write-access to the processor and to the desired data file or process within the processor. Penetration may be accomplished by defeating identification and authentication mechanisms or by inserting malicious code into a legitimate transaction.

(c) **Connection integrity issues:** Successful implementation of e-government services requires some degree of confidence on the part of private citizens or other user entities that information being read originated only with the assumed government source and that information being provided goes only to the appropriate government destination(s).

3. **Confidentiality**

Confidentiality protection is protection against disclosure of information without the implicit or explicit consent of an entity that legitimately possesses the information

(a) **Impacts or consequences of unauthorized exposure:** The consequences of unauthorized exposure of information via e-government resources depend in large part on the specific information that is exposed.

(b) **Loss of confidence in institutions and service delivery mechanisms:** Public disclosure of e-government confidentiality breaches can result in loss of public confidence in e-government mechanisms and in the institutions that they serve. The future of e-government will be determined in large part by public acceptance of e-government mechanisms as a dependable approach to doing business with governments.

Some Other Threats

- **Malicious codes:** Computer viruses, worms and Trojan Horses are examples of malicious code. People are aware but may not be prepared to deal with such adversaries.
- **Communication channel threats:** The Internet serves as the electronic chain linking a consumer (client) to the e-Gov server. Messages on the Internet travel randomly from a source node to a destination node. It is impossible to guarantee that every computer on the Internet through which messages pass is safe, secure, and non-hostile.
- **Server threats:** The server is the third link in the client-Internet-server trio embodying the e-Gov path between the citizens and the government. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information.

- **Web server threats:** Web server software is not inherently high-risk, it has been designed with Web service and convenience as the main design goal. The more complex the software is, the higher the probability that it contains coding errors (bugs) and security holes.
- **e-Gov server threats:** The e-Gov server, along with the Web server, responds to requests from Web browsers through the HTTP protocol and Common Gateway Interface (CGI) scripts. Several pieces of software comprise the egov server software suite. Each of these softwares can have security holes and bugs.
- **Database threats:** Besides government information, databases connected to the Web contain critical and private information that could irreparably damage a enterprise or citizen if it were disclosed or altered. Some databases store user name/password pairs in a non-secure way. If someone obtains user authentication information, then he or she can masquerade as a legitimate database user and reveal private and costly information.
- **Password hacking:** The simplest attack against a password-based system is to guess passwords. Guessing of passwords require access to the complement, the complementation functions, and the authentication functions be obtained. If none of these have changed by the time the password is guessed, then the attacker can use the password to access the system.

Security Approaches for E-Government

1. Cryptographic Mechanisms

Cryptography – Cryptography is another best method in security. They give the power to hidden the information during the network traverse or stored. In which many methods has to purpose like 16-bit, 32-bit, 128-bit, 256-bit encryption or many algorithms like DES, AES, Message Digest, RSA, Quantum encryption etc. In these methods the original message (called plain text) is converted in non-readable form. For example that if plain text is 100 bit long and want to send this information to another person through network then we will add the extra bit in the plain text like 28-bit if we are using the 128-bit encryption method using the public/private key according to the algorithm after that is message is converted into non-readable (called cipher text) from and send it into a network or stored. Information is received by receiver, they firstly decrypt the information again using the public/private key, and decryption is the just reverse process of the encryption.

2. Database Design

Some e-government services include provision of data that are derived from aggregation or analysis of information that is subject by law to privacy protection, are proprietary, or for which confidentiality must otherwise be maintained. A number of database design and management approaches have been developed to address this problem.

3. **Anti-virus system:** When we discuss about digital threats the first thing in our mind is virus, which affects our ICT assets in various ways such as- slowing down of the system, occupy disk space, corrupt our valuable data or storage medium etc. it is also known as malware, worms and Trojan horses. there are "over 1,122,311 known viruses active in the world as of 2008".

4. **Firewalls**

"A system designed to prevent unauthorized access to or from a private network[3]". A firewall is a security device that can be hardware or software that is mainly use for to separate a secure area from a less secure area and to control communications between the two. We have several firewall techniques such as Packet filter, Application gateway, Circuit-level gateway, Proxy server. There are many different brands of software firewalls, some of them are ZoneAlarm, BlackICE and Kerio etc.

5. **Analysis tools**

There is strong need for analysis tool because of the increasing sophistication of attacker rules and the bugs/errors/loopholes present in the used applications/system, it is very important to review periodically network loopholes to compromise. A multiple range of loopholes/bugs identification tools are present, which give the command and take the advantage to analysis the network. Analysis tools are freely available to the internet they give the advantage to analysis the network and find the threat and misused the treat for attack on the network.

6. **Monitoring tools**

Regular monitoring of network activity is essential if a web portal is to maintain a highly confidential data on the network. Network monitoring tools should be installed at appropriate location for collecting and regularly monitor the network and examine the data traveled in the network for any suspicious activity from the attackers. Presently it's possible in various monitoring tools providing the automatic alert system means when they found any suspicious activity in network than the issue a notification to network administrator. Most of attacker used the denial-of-service attack because the administrator is busy to solve this problem and they hack all the confidential information/data form the network or place a malicious code in the network they give regularly information to the attacker and send a copy of all the data or information automatically without knowledge to the administrator.

7. **Biometric technology**

Biometric technology is process of verifying or identifying an person with two different approaches is (1) physiological characteristic, in which examine the fingerprint, IRIS examine or face detection, (2) behavioral characteristic, in which check the keystroke, dynamic signature or voice verifications. They both are included in the biometric technology. Biometric technology is one of the best security mechanism for secure our private or confidential data from the attacker or various malicious activities.

https://www.ijert.org/research/enhance-security-system-of-e-governance-IJERTV2IS90486.pdf

E-Governance Present Security System

In the e-governance security system is also work as on the old system of security. Here which only prescribed the advanced security system but that is not presently in working. If the e-governance is want to upgrade the our security system with high level of security system, high level of security system implemented with the help of biometric scanning. If the e-governance is used the biometric system of the UID then the e-governance system is going to secure. But presently two different stages is that a. Registration or Login b. One-time Password (OTP)

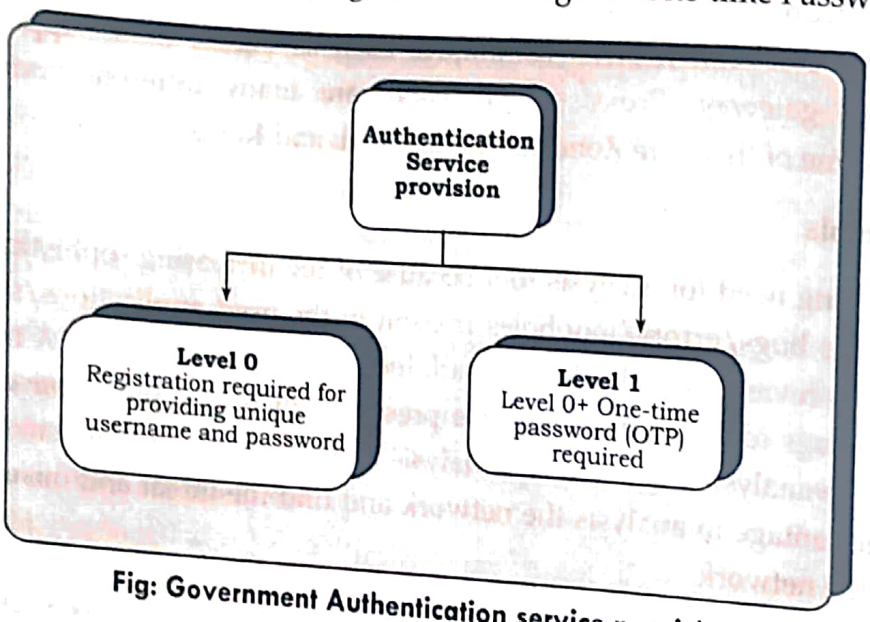


Fig: Government Authentication service provision

Registration or Login – In this process, if the user is login at first time then they will required to registrated him/her self with the help of registration form and give the some basic details like name, address, mobile no etc. this information is not verified by the system and user will easy going to registred on the web portal and access all the information. if user is already registered on this web portal then his/her required the fill the user name and password that is given at the time of registration and after that he/she will be able to access all the government information directly.

One-time Password – At present the e-governance is made a different web portal with the name of eparmaan. In the e-parmaan portal firstly the user will required to registered him/her self with the basic information and also a another option is One-time password. It's meaning that after fill all the information, one tempary password is send on the user's mobile no that is entered at time of registraion. This password is alive only for 3-5 mint. After that this is automatically dead. This is just a system generated password with 4-5 digit. Each in every time the password is changed. After receiving the password the user will be able to work with our login. The beniftit of this process at-leat the user's mobile is verified by the system.

Enhancement of Security System of E-Governance

Registration and Authentication

Registration is the process for access restricted services/document. Registration and authentication process is both are implemented parallel at the same time. Actually the major differences between the both the process is that the registration process the user is give the personal information like name & password for login, E-mail id, address, mobile no etc. But in the authentication process verify that this information is correct and the information is not used by another person. When these processes is implementing on internet it's called "Electronic authentication (eauthentication)". Electronic authentication is achieved by the following factors:

- Knowledge - something the user knows (e.g. user name, password, PIN, secret questions and answers, etc.);
- Possession - something the user has (e.g. Digital signature, smart card, etc.);
- Be - something the user is (e.g. biometric fingerprint, iris pattern, face recognition etc.); or - A combination of the above. E-authentication service is implemented in different level. Here we give the different level of authentication service is that?

Authentication Service Provision

Level 0: This is the basic authentication mechanism using username and password. The user could be provided the capability of self-registration by which he/she can generate a username/password. He/she fill the self-registration form with the basic information also including the authenticated information like Aadhaar, PAN, Driving License, Rashan Card no etc. all this information helpful, if the user will forgot your username/password.

Level 1: At Level 1, a user will be able to prove her identity using OTP token along with his/her Unique Identification Card number (UID) credentials. The OTP will provide on his/her mobile phone no, this is entered at the time of registration of UID [6].

Level 2: At Level 2, the user would need to prove his/her identity through a hardware or software token (along with PIN). For this purpose, token would be a digital certificate/digital signature or a smart card or personal identification number (PIN) issued by the higher authority that would be required from the login.

Level 3: At Level 3, the user will prove his/her identity using biometrics authentication. This is the highest level of authentication security that would be available to a user. Biometrics based verification would be done in accordance with the Aadhaar authentication process.

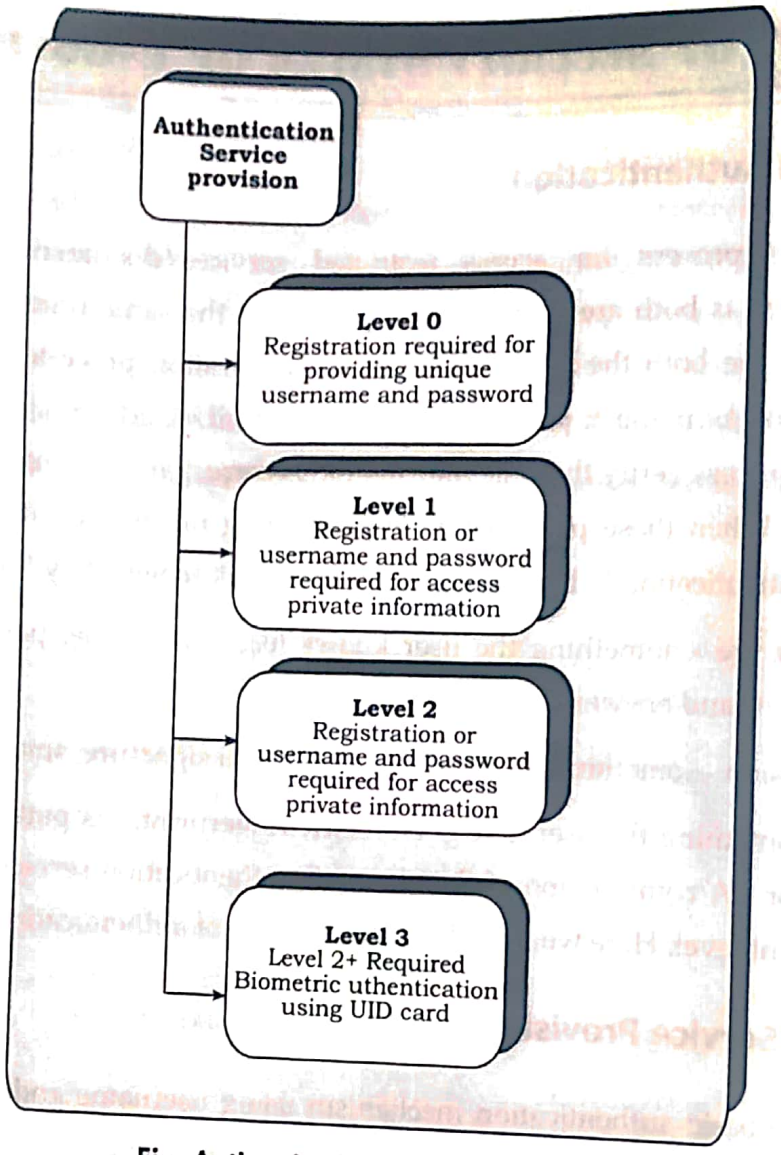


Fig: Authentication Service Provision

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". A security model is a generic blueprint offered by a service organization Think of it as an 'approach' or 'strategy' that you may use as a starting point and modify to fit the needs of your organization Some security models are proprietary, some are inexpensive (ISO-27K), some are free (NIST)

1. **Access Control Models**

   Access controls regulate the admission of users into trusted areas of the organization— both the logical access to the information systems, or the physical access to the organization's facilities

Access control is maintained by means of a collection of policies, programs to carry out those policies, and technologies that enforce policies

- 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)
- Access control is built on several key principles:
  - Least privilege: The principle by which members of the organization can access the minimum amount of information for the minimum amount of time necessary to perform their required duties
  - Need to Know: Limits a user's access to the specific information required to perform the currently assigned task, and not merely to the category of data required for a general work function
  - Separation of Duties: 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 Controls

- Directive—Employs administrative controls such as policy and training designed to proscribe certain user behavior in the organization
- **Deterrent:** Discourages or deters an incipient incident
- **Preventative:** Helps an organization avoid an incident
- **Detective:** Detects or identifies an incident or threat when it occurs
- **Corrective:** Remedies a circumstance or mitigates damage done during an incident
- **Recovery:** Restores operating conditions back to normal
- **Compensating:** Resolves shortcomings

	Deterrent	Preventive	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	Warming signs	Gates, fences, and guards	Sentries, CCTVs	Fire suppression systems	Disaster recovery procedures	Defense in depth
Technical	Warming banners	Login systems, kerberos	Log monitors and IDPSs	Forensics procedures	Data backups	Key logging and keystroke monitoring

a) **NIST Control Categories**

- **Management:** Controls that cover security processes that are designed by strategic planners, integrated into the organization's management practices, and routinely used by security administrators to design, implement, and monitor other control systems
- **Operational (or Administrative):** Controls that deal with the operational functions of security that have been integrated into the repeatable processes of the organization
- **Technical:** Controls that support the tactical portion of a security program and that have been implemented as reactive mechanisms to deal with the immediate needs of the organization as it responds to the realities of the technical environment

b) **Mandatory Access Controls (MACs)**

- A Mandatory Access Control (MAC) is required and is 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 or classification levels
- When MACs are implemented, users and data owners have limited control over access to information resources

c) **Data Classification Model**

- Data owners must classify the information assets for which they are responsible and review the classifications periodically
- The U.S. military classification scheme relies on a more complex four-level classification scheme as defined in Executive Order 13526. There are three levels of classified data, and then unclassified:
  - Top Secret Data
  - Secret Data
  - Confidential Data
  - Unclassified Data
- Simple scheme for other organizations:
  - Public
  - For official (or internal) use only
  - Confidential (or Sensitive)

d) **Security Clearances Structure**

- In a security clearance structure, each user of an information asset is assigned an authorization level that indicates the highest level of information classification they may access
- Most organizations have developed roles and corresponding security clearances so individuals are assigned into authorization levels correlating with the classifications of the information assets

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

e) **Managing Classified Information Assets**

- Managing an information asset includes all aspects of its life cycle—from specification to design, acquisition, implementation, use, storage, distribution, backup, recovery, retirement, and destruction
- An information asset that has a classification designation other than unclassified or public must be clearly marked as such - with a cover page and headers & footers
- To maintain the confidentiality of classified documents, managers can implement a clean desk policy- requiring employees to secure all information in an appropriate storage container at the end of each business day
- When copies of classified information are no longer valuable or too many copies exist, care should be taken to destroy them properly to discourage dumpster diving
- While bins stored on private property can be protected from trespassers, in 1998, the Supreme Court ruled that there is no expectation of privacy for items thrown away in trash or refuse containers

f) **Lattice-Based Access Controls**

- A variation on the MAC form of access control, Lattice-Based Access Controls assigns users a matrix of authorizations for particular areas of access
- The level of authorization may vary depending on the classification authorizations that individuals possess for each group of information assets or resources
- The lattice structure contains subjects and objects, and the boundaries associated with each subject/object pair are clearly demarcated

g) **Nondiscretionary Controls**

- Nondiscretionary controls are determined by a central authority in the organization and can be based on roles—called role-based access controls or RBAC—or on a specified set of tasks—called task-based controls
- Role-based controls are tied to the role that a particular user performs in an organization, whereas task-based controls are tied to a particular assignment or responsibility

h) **Discretionary Access Controls (DACs)**

- Discretionary Access Controls (DACs) are implemented at the discretion or option of the data user
- Users can allow general, unrestricted access, or they can allow specific individuals or sets of individuals to access these resources

- Most personal computer operating systems are designed based on the DAC model
- One discretionary model is rule-based access controls where access is granted based on a set of rules specified by the central authority

i) **Other Forms of Access Control**

- **Content-dependent access controls:** As the name suggests, access to a specific set of information may be dependent on its content (e.g. Accounting information for the Accounting Department)
- **Constrained user interfaces**: Some systems are designed specifically to restrict what information an individual user can access (e.g. ATMs)
- **Temporal (time-based) isolation:** In some cases, access to information is limited by a time-of-day constraint (e.g. Time-release safes)

2. **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

Trusted Computing Base

- Trusted Computer System Evaluation Criteria (TCSEC)
  - U.S. Government Department of Defense standard that defines criteria for assessing access controls in a computer system
  - Part of a larger series of standards collectively referred to as the Rainbow Series, due to the color-coding used to uniquely identify each document
- Also known as the "Orange Book" and is considered the cornerstone of the series
- Trusted computing base (TCB)
  - The combination of all hardware, firmware, and software responsible for enforcing the security policy
- In this context, security policy refers to the rules of configuration for a system, rather than a managerial guidance document
  - Made up of the hardware and software that has been implemented to provide security for a particular information system
- Reference monitor
  - A conceptual object
  - The piece of the system that manages access controls

- It mediates all access to objects by subjects
  - Systems administrators must be able to audit or periodically review the reference monitor to ensure it is functioning effectively, without unauthorized modification
- Covert channels
  - Unauthorized or unintended methods of communications hidden inside a computer system
  - Types of covert channels
  - Storage channels, which communicate by modifying a stored object
  - Timing channels, which transmit information by managing the relative timing of events

3. Bell-LaPadula Confidentiality Model

- A state machine model that helps ensure the confidentiality of an information system
  - Using mandatory access controls (MACs), data classification, and security clearances
  - A state machine model follows a conceptual approach in which the state of the content of the system being modeled is always in a known secure condition
  - This kind of model is provably secure
- A system that serves as a reference monitor compares the level of classification of the data with the clearance of the entity requesting access
  - It allows access only if the clearance is equal to or higher than the classification
- BLP security rules prevent information from being moved from a level of higher security level to a level of lower security

Access modes can be one of two types

- **Simple security**
  - Prohibits a subject of lower clearance from reading an object of higher classification, but allows a subject with a higher clearance level to read an object at a lower level (read down)
- The * (star) property
  - The * property (the write property) prohibits a high-level subject from sending messages to a lower-level object
- Subjects can read down and objects can write or append up

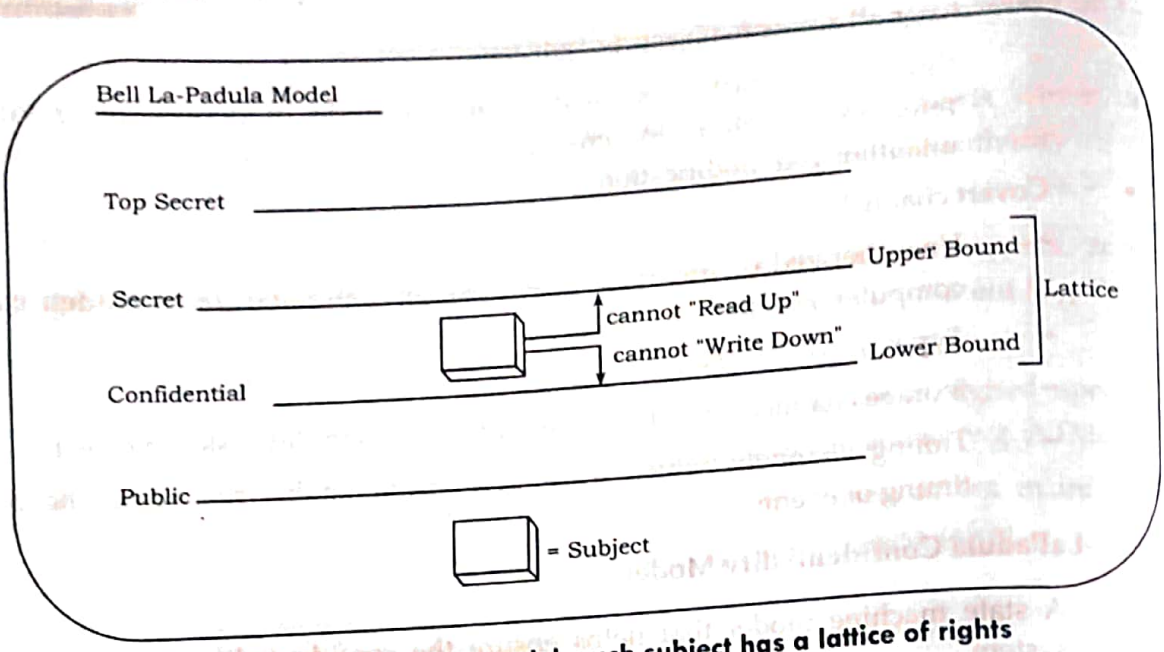
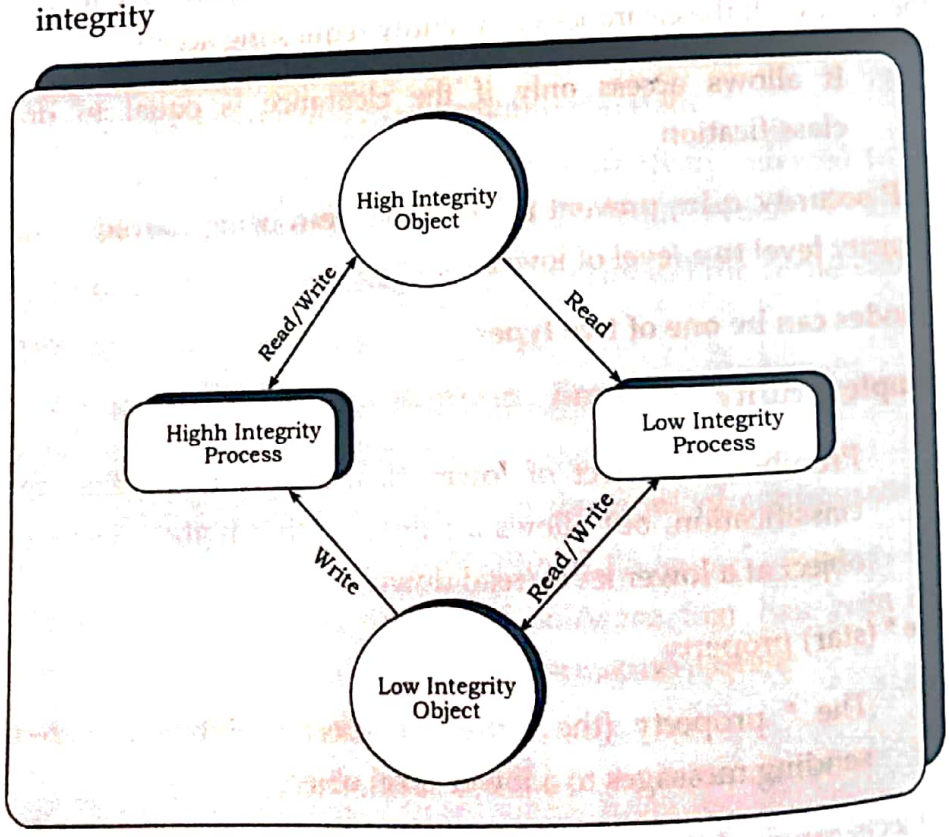


Fig: In the Bell-LaPadula model, each subject has a lattice of rights

5.

4. Biba Integrity Model

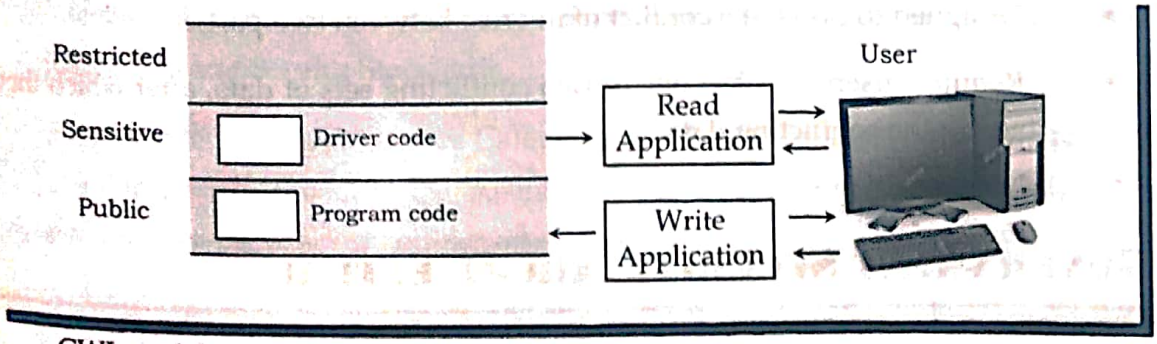
- Similar to Bell-LaPadula
- Provides access controls to ensure that objects or subjects cannot have less integrity as a result of read/write operations
- Ensures no information from a subject can be passed on to an object in a higher security level
  - This prevents contaminating data of higher integrity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



- Assigns integrity levels to subjects and objects using two properties
  - The simple integrity (read) property
- Permits a subject to have read access to an object only if the security level of the subject is equal to or lower than the level of the object.
  - The integrity * (write) property
- Permits a subject to have write access to an object only if the security level of the subject is equal to or higher than that of the object.

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
- Establishes a system of subject-program-object relationships
  - Such that the subject has no direct access to the object
  - The subject is required to access the object using a well-formed transaction using a validated program
  - Provides an environment where security can be proven through separated activities, each of which is provably secure



- CWI model controls
  - Subject authentication and identification
  - Access to objects by means of well-formed transactions
  - Execution by subjects on a restricted set of programs
  - Elements of the CWI model
  - Constrained data item (CDI)

- The integrity of this data item is protected

6. **Graham-Denning Access Control Model**

- Composed of three parts
  - A set of objects
  - A set of subjects (a process and a domain)
- The domain is the set of constraints controlling how subjects may access objects
  - A set of rights
- Primitive protection rights
  - Create or delete object, create or delete subject
  - Read, grant, transfer and delete access rights

7. **Harrison-Ruzzo-Ullman 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

8. **Brewer-Nash Model (Chinese Wall)**

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

E-GOVERNMENT SECURITY ARCHITECTURE

The security architecture of E-governance is a high level document that set the security goals of e-governance project and describe the procedure that need to be followed by all the e-governance hierarchy such as users, businesses, operators etc. Appropriate legal framework is absolutely essential for the systematic and sustained growth of e-governance.

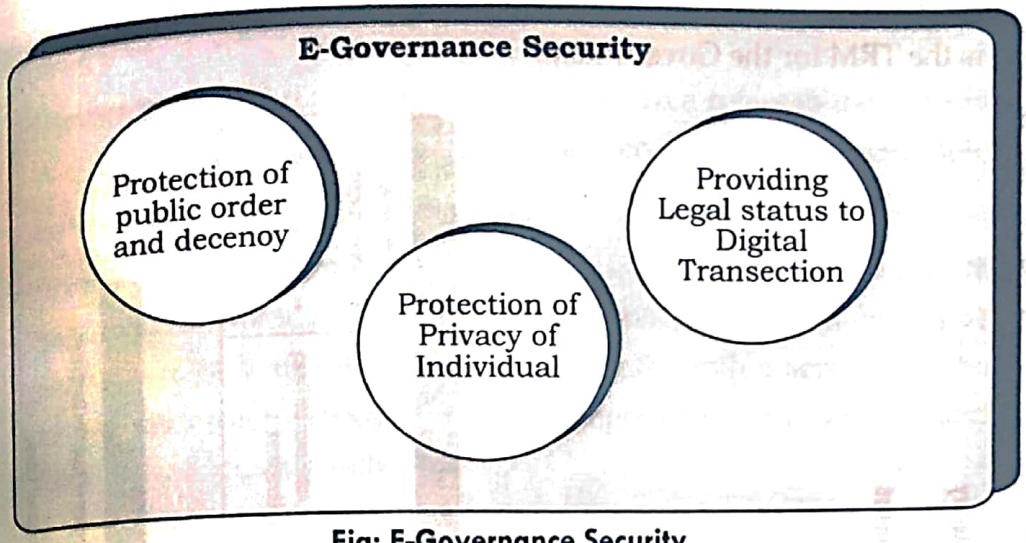


Fig: E-Governance Security

E-Government Security Architecture Reference Framework

e-Government Security Architecture forms part of the Technical Reference Model (TRM). TRM supports and enables the delivery of ICT Security Standards Domains and capabilities and provides a foundation to advance the re-use and standardization of technology and service components from a Government-wide perspective. Aligning ICT capital investments to the TRM leverages a common, standardized vocabulary allowing cross departmental discovery, collaboration and interoperability. Public Institutions will benefit from economies of scale by identifying and re-using the best solutions and technologies to support their business functions, missions and target architecture. The TRM will continue to evolve with the emergence of new technologies and standards.

The TRM has been structured hierarchically as:

i. **Service area:** Each Service Area aggregates the standards and technologies into a lower-level functional area. Each Service Area consists of multiple Service Categories and Service Standards.

ii. **Service category:** Each Service Category classifies lower levels of technologies and standards with respect to the business or technology function they serve. In turn each Service Category is comprised of one or more service standards.

iii. **Service standards:** They define the standards and technologies that support a Service Category. To support Public Institutions mapping into the TRM, many of the Service Standards provide illustrative specifications or technologies as examples.

The following is the TRM for the Government.

Fig: Technical Reference Model

The TRM is standardised under 4 service areas:

i. **Service Access and Delivery:** This service area refers to the collection of standards and specifications to support external access, exchange and delivery of Service Components or capabilities.

ii. **Service Interface and Integration:** This service area refers to the collection of technologies, standards, and specifications that govern how Public Institutions shall interface both internally and externally with a service component. This area also defines the methods by which components shall interface and integrate with back-office/ legacy assets.

iii. **Service Component Framework:** This service area refers to the underlying foundation, technologies, standards, and specifications by which Service Components are built, exchanged, and deployed across Distributed or Service-Orientated Architectures.

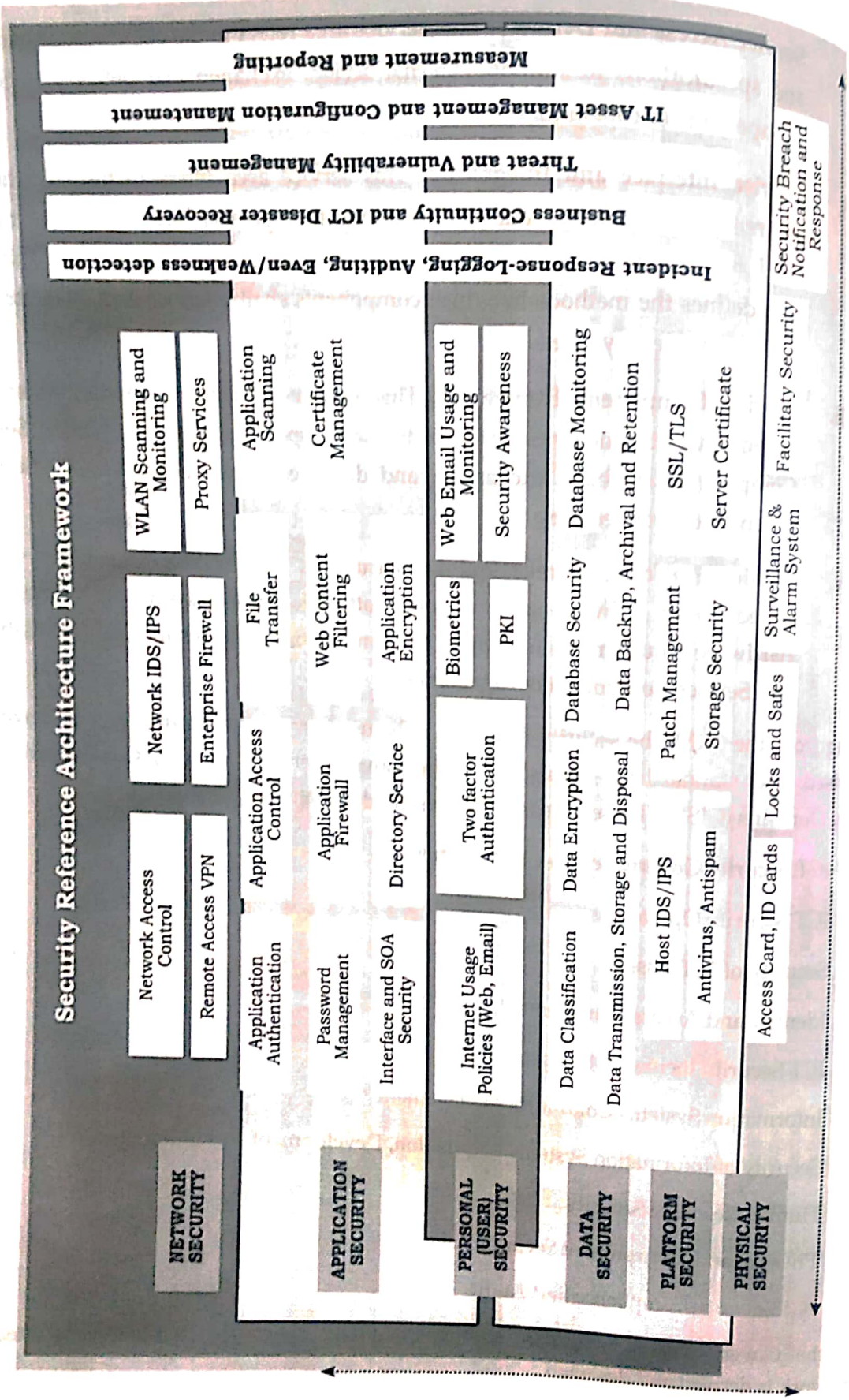
iv. **Service Platform, Storage and Infrastructure:** This service area refers to the collection of delivery and support platforms, infrastructure capabilities and hardware requirements to support the construction, maintenance, and availability of a Service Component or capabilities.

Deriving from the TRM, the security measures to be used across the security layers above are categorised and standardised across the entire Government in ten (10) Government ICT Security Domains (GISD). These domains are presented below:

1. ICT Security Governance and Management
2. ICT Security Operations
3. Security of ICT Assets
4. Identity and Access Management
5. ICT Security Incident Management
6. Information Systems Continuity Management
7. Security of Information Systems Acquisition, Development and Maintenance
8. Human Resource Security
9. Physical and Environment Security
10. ICT Security Compliance and Audit

From the Government ICT Security Domains (GISD), a security Reference Architecture Framework is derived and designed.

Security Reference Architecture Framework



The above are details of the core layers described in Figure II.

Table I: Details of the core layers described in Security Reference Architecture Framework

Security Layers Description

- **Network Security:** Network security deals with the security mechanisms adopted for the network considering network local/remote access control, authentication, firewall protection, network intrusion detections, and security administration used by the Public Institution's ICT Operations and users
- **Application Security:** Application security is the use of software, hardware, and procedural methods to protect applications from external threats. Security measures built into applications and a sound application security routine minimize the likelihood that hackers will be able to manipulate applications and access, steal, modify, or delete sensitive data.
- **Personnel/User Security:** User security deals with the various aspects of security mechanism enforced at the end user level. It focuses on the user internet usage policies to be enforced and monitored, the various authentication mechanisms for verification of user identify such as two-factor authentication, biometrics based authentication, increase security awareness among users and employees and conduct security training.
- **Data Security:** Data security deals with security mechanism adopted for keeping data protected from corruption and unauthorized access to ensure data privacy while maintaining data confidentiality. Data is considered a primary asset and as such shall be protected in a manner commensurate to its value. Security and privacy shall focus on controlling unauthorized access to data.
- **Platform /Host Security:** Platform security deals with the security mechanisms adopted on servers, workstations and operating systems. It covers server access control, host intrusion detections, use of server and desktop based anti-virus, anti-spyware, software patch management, storage security, IP security, communications endpoint security etc.
- **Physical Security:** Physical security refers to the security characteristics concerned with restricting physical access by unauthorized personnel (potential intruders) to controlled facilities (buildings, computer rooms, data centres etc.) along with the access systems and types of access controls used in those same facilities or sites.

Cross Pillars

- **Incident Response:** Incident Response aims to address and manage any security breach or attack.
- **Business Continuity and ICT Disaster Recovery:** Business Continuity and ICT Disaster Recovery describes the process and procedures a Public Institution will put in place to ensure that essential business functions and ICT operations can continue during and after a disaster.

- **Threat and Vulnerability Management:** Threat and vulnerability aims to identify risks and mitigation control in the ICT environment.
- **ICT Asset Management:** ICT Asset management is a set of business practices to manage ICT assets throughout their lifecycle.
- **Measurement and Reporting:** Measurement and reporting provides information on the health check of the ICT appliances and systems.

The core layers described in the Figure II diagram of the Security Architecture have been mapped against 10 defined Government ICT security domains (GISD) as follows:

Table II: Defined Government ICT Security domains (GSD)

ICT Security Domain	Security Layers
1. ICT Security Governance and management	Cross pillars: Measurement and Reporting
2. ICT Security Operations	Network security, application security, data security, platform/host security
3. Security of ICT Assets	Cross pillars: ICT asset management
4. Identity and Access Management	Network security, application security, physical security
5. ICT Security Incident Management	Cross pillars: Incident response
6. Information System Continuity Management	Cross pillars: Business Continuity and ICT Disaster recovery, threat and vulnerability management
7. Security of Information Acquisition, Development and Maintenance	Application security
8. Human Resource Security	Personal/user security
9. Physical and Environment Security	Physical security
10. ICT Security Compliance and Audit	Cross-pillars: Measurement and Reporting

SECURITY STANDARD

Security Standard represents a set of requirements that a product or a system must achieve. Assuming the conformity of a product or system with a certain standard demonstrates that it fulfills all the standard's specifications. There are currently some primary standards in place governing information security.

...ed of Security Standard

...e use of standards is unanimously accepted and gives the possibility of comparing a personal ...curity system with a given frame of reference adopted at an international level. A good ...ample is the ISO 9000 set of standards regarding the quality management system, which is a ...common reference regardless of the industry in which a certain company activates. Standards ...sure desirable characteristics of products and services such as quality, safety, reliability, ...ficiency and interchangeability - and at an economical cost. We need information security ...andards in order to implement information security controls to meet an organizations ...quirements as well as a set of controls for business relationships with other organizations and ...e most effective way to do this is to have a common standard on best practice for information ...curity management such as ISO/IEC 17799:2005. Organizations can then benefit from ...mmon best practice at an international level, and can prove the protection of their business ...ocesses and activities in order to satisfy business needs.

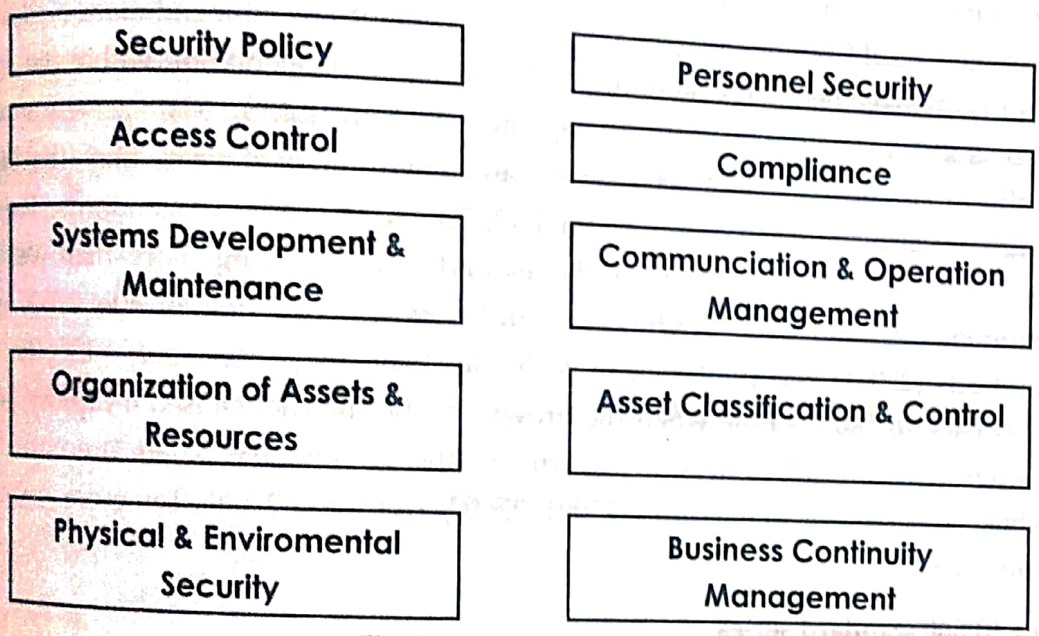


Fig: Major Security Areas

Some of Security Standards

1. **The ISO/IEC 27000 standards series**

The International Organization for Standardization (Organization internationale de normalization), known as ISO, is an international-standard-setting body composed of representatives from various national standards organizations. Founded on 23 February 1947, the organization promulgates world-wide proprietary industrial and commercial standards. ISO's headquarters are in Geneva, Switzerland ISO is defined as a non-governmental organization, but its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most non-governmental organizations. The ISO International Standards are published in accordance with the following format: ISO[/IEC][/ASTM] [IS] nnnnn[:yyyy] Title, where

nnnnn is the number of the standard, yyyy is the year published, and Title describes the subject. IEC stands for International Electrotechnical Commission and is included if the standard results from the work of ISO/IEC JTC1 (the ISO/IEC Joint Technical Committee). For standards developed in cooperation with ASTM International, ASTM is used. ISO has 157 national members, out of the 195 total countries in the world. ISO has three membership categories: Member bodies are national bodies that are considered to be the most representative standards body in each country. These are the only members of ISO that have voting rights. Correspondent members are countries that do not have their own standards organization. These members are informed about ISO's work, but do not participate in standards promulgation. Subscriber members are countries with small economies. They pay reduced membership fees, but can follow the development of standards. The ISO/IEC 27000-series (also known as the 'ISMS Family of Standards' or 'ISO27k' for short) comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The series provides recommendations on information security management, risk handling and controls implementation within the context of an overall Information Security Management System (ISMS). Management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series) are also similar in design to the ISO/IEC 27000- series of standards. The series is applicable to organizations of all shapes and sizes covering more than just privacy, confidentiality and IT or technical security issues. The first of the 27000 series of standards (27001) was published in 2005. However, its predecessor -- ISO/IEC 17799 - dates back to 2000, a time when the growth of the Internet caused a rapidly increasing awareness of the importance of security in the IT industry. There are currently four published standards in the series: 27001, 27002, 27005 and 27006. Ten more are at various draft stages.

3.

2. The SP800 standard series

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve the quality of life. NIST has a total budget of $931.5 million and employs about 2,900 scientists, engineers, technicians, and support and administrative personnel. 2 NIST Laboratories provide measurements and standards for U.S. industry:

- Building and fire research
- Chemical science and technology
- Electronics and electrical engineering
- Information technology

- Manufacturing engineering
- Materials science and engineering
- Nanoscale science and technology
- Neutron research
- Physics
- Technology services

Established in 1990 the NIST Special Publications 800 group of documents is the oldest of all the information security standards. It consists of over a hundred documents covering almost every aspect of information security. The most representative among all these documents is the computer security handbook SP800- 12 which provides a good idea of the NIST approach.

ISF Standard of Good Practice for Information Security

The Information Security Forum (ISF) is an international, independent, non-profit organization dedicated to benchmarking and best practices in information security. It was established in 1989 as the European Security Forum but expanded its mission and membership in the 1990s, so that it now includes hundreds of members, including a large number of Fortune 500 companies, from North America, Asia, and other locations around the world. Groups of members are organized as chapters throughout Europe, Africa, Asia, the Middle East, and North America. The ISF is headquartered in London, England, but also has staff based in New York City. The membership of the ISF is international and includes large organizations in transportation, financial services, chemical/ pharmaceutical, manufacturing, government, retail, media, telecommunications, energy, transportation, professional services, and other sectors. The Standard of Good Practice (SoGP) was first released in 1996 by the Information Security Forum (ISF) and it represents a detailed documentation of best practice for information security. The Standard is published and revised biannually. Standard of Good Practice, which is freely available, derives from the ISO/IEC 27002 and COBIT v4.1. standards and outlines a functional information security methodology based on both research and real world experience. The standard is centered around the following six key aspects: 1. Computer installations. This aspect is targeted chiefly at IT specialists, and addresses the hardware and software that supports the critical business applications. 2. Critical business applications. These are the applications on which the organization's activities depend. This aspect is primarily targeted at the CBA owners, the individuals in charge of business processes and systems integrators. 3. Security management. The security management aspect is targeted at security decision makers and auditors. It handles management level decision making in relation to security implementations across the organization. 4. Networks. Networks form a special category due to their unique security vulnerabilities. Its target is typically network managers, network service specialists and network service providers. The network aspect addresses the nature and implementation of an

organization's networking requirements. 5. Systems development. This aspect addresses to system developers and deals with the identification, design and implementation of system requirements. 6. End user environment. The end user environment is the point at which individuals are using the organization's systems and applications to support business processes. This aspect therefore tends to target business managers and individuals who work within such end user environments.

4. Control Objectives for Information and related Technology (COBIT)

The ISACA (Information Systems Audit and Control Association) was founded in the USA in 1967 by a group of individuals dealing with auditing controls in the computer systems, when they realized the need for a standard in the field. In 1969, Stuart Tyrnauer founded an entity named EDP Auditors Association. In 1976 the association developed as an education foundation with the scope of expanding the knowledge and value of the IT governance and control field. Today, ISACA's membership is composed of more than 75,000 members worldwide. Members live and work in more than 160 countries and cover a variety of professional IT-related positions. The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information technology management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI). COBIT was first released in 1996. Its mission is "to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors." COBIT helps Managers, auditors, and other users to understand their IT systems and decide the level of security and control that is necessary to protect their companies' assets through the development of an IT governance model. COBIT is an IT governance framework that allows managers to fill in the gap between control requirements, technical issues and business risks. The latest update COBIT 4.1 helps organizations to increase the value attained from IT, highlights links between business and IT goals, and simplifies implementation of the COBIT framework. COBIT 4.1 is a fine-tuning of the COBIT framework and can be used to enhance work already done based upon earlier versions of COBIT. COBIT 4.1 has 34 high level processes that cover 210 control objectives categorized in four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring and Evaluation: 1. Plan and Organize. The Plan and Organize domain describes how IT can be used to help achieve the company's goals and objectives. 2. Acquire and Implement. This domain covers activities such as identifying IT requirements, acquiring the technology, and implementing it within the company's current business processes. 3. Deliver and Support. It covers areas such as the execution of the applications within the IT system and its results, as well as, the processes that enable the efficient execution of these IT systems. 4. Monitor and Evaluate. This domain deals with the strategy of assessing the needs of the company and establishes whether or not the current IT system still meets the objectives for which it was designed. 1. COBIT and ISO/IEC 27002 do not compete with each other and actually complement one another. COBIT typically covers a broader area than ISO/IEC 27002.

BSI IT-Grundschutz - IT baseline protection

The Bundesamt für Sicherheit in der Informationstechnik (abbreviated BSI - in English: Federal Office for Information Security) is the German government agency in charge of managing computer and communication security for the German government. Its areas of expertise and responsibility include the security of computer applications, critical infrastructure protection, Internet security, cryptography, counter eavesdropping, certification of security products and the accreditation of security test laboratories. It is located in Bonn and has over 400 employees. BSI's predecessor was the cryptographic department of Germany's foreign intelligence agency (BND). BSI still designs cryptographic algorithms such as the Libelle cipher. The BSI Standards contains recommendations on methods, processes, procedures and approaches relating to information security. For accomplishing that the BSI standards contains fundamentally important areas for information security regarding public authorities and companies and for which appropriate practical approaches have been established. BSI Standard 100-1 is the first standard of the BSI IT-Grundschutz series and defines the general requirements for implementing an ISMS. It is completely compatible with ISO Standard 27001 and also takes into consideration the recommendations within ISO Standards 13335 and 27002. BSI-Standard 100-2 also known as The IT-Grundschutz Methodology is a step by step description of how IT security management can be set up and operated in practice. The IT-Grundschutz Methodology provides a detailed description of how to select appropriate IT security measures, how to produce a practical IT security concept, and how to implement the IT security concept. IT-Grundschutz interprets the general requirements of the ISO Standards 27001, 27002 and 13335 and provides many notes, background expertise and examples in order to help users implement them in practice. The IT-Grundschutz Catalogues not only explain what has to be done, they also provide very specific information as to what implementation may look like. BSI-Standard 100-3: The third standard from the BSI series deals with a method of risk analysis based on IT-Grundschutz. This approach can be used when organizations are already working successfully with the IT-Grundschutz Manual and would like to add an additional risk analysis to the IT- Grundschutz analysis.

DISCUSSION EXERCISE

1. Explain Security in E governance.
2. What are the Challenges and Approach of E-Government Security
3. Explain various threats of E governance.
4. Explain various Security Management Model briefly.
5. What is Security Standards and its need.
6. Explain some of Security Standards.
7. Short notes:
   a. Biba Integrity Model
   b. Clark Wilson Model

❑❑❑