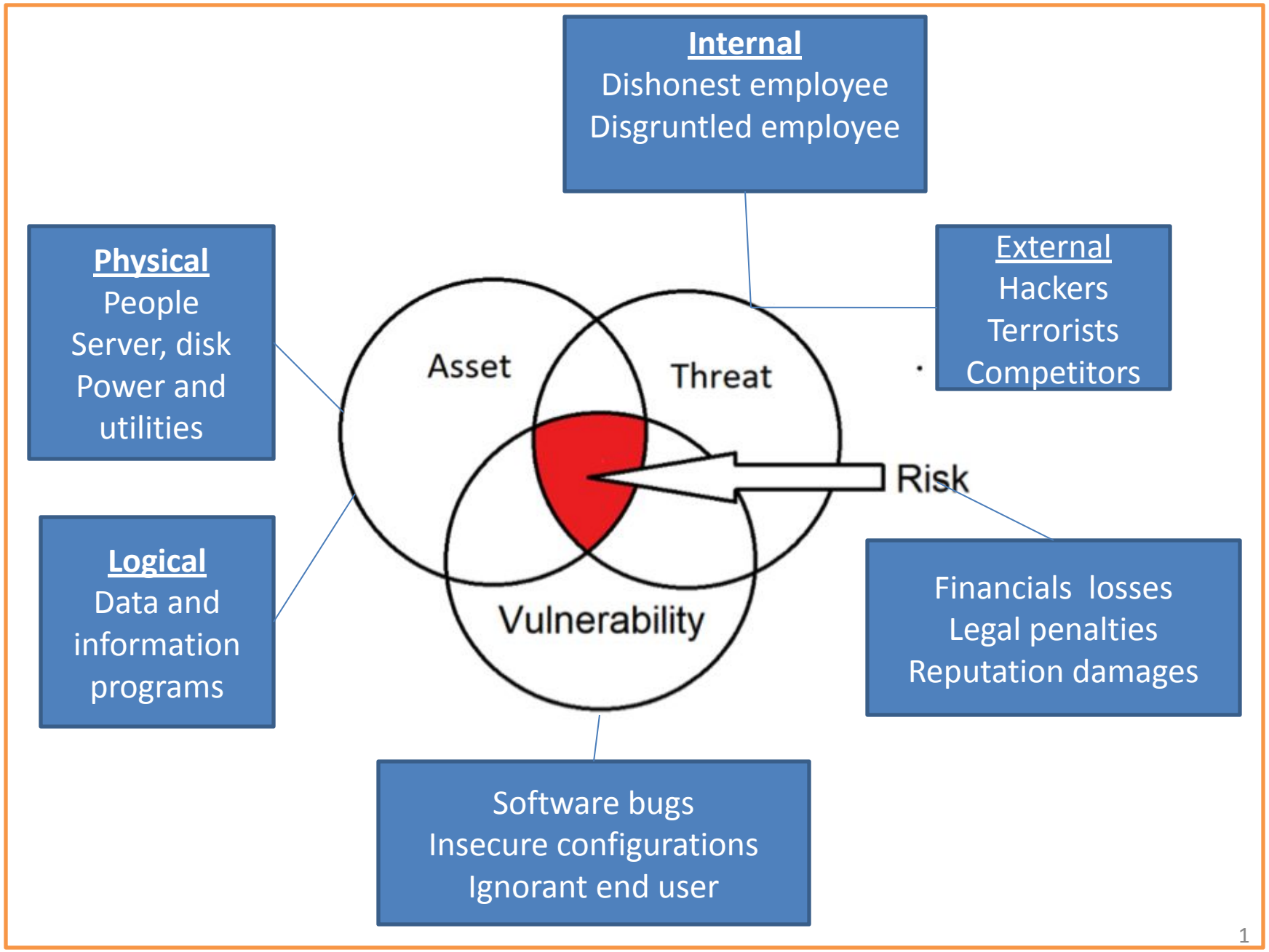

Internal
Dishonest employee
Disgruntled employee
Physical
People
Server, disk
Power and utilities
External
Hackers
Terrorists
Competitors
Asset
Threat
Risk
Logical
Data and information programs
Vulnerability
Financials losses
Legal penalties
Reputation damages
Software bugs
Insecure configurations
Ignorant end user

- **Vulnerability**
  - Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack.
  - A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.
- **Threat**
  - In Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.
- **Risk**
  - A probability or threat of damage, injury, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided / minimized through preemptive action

Control of information system

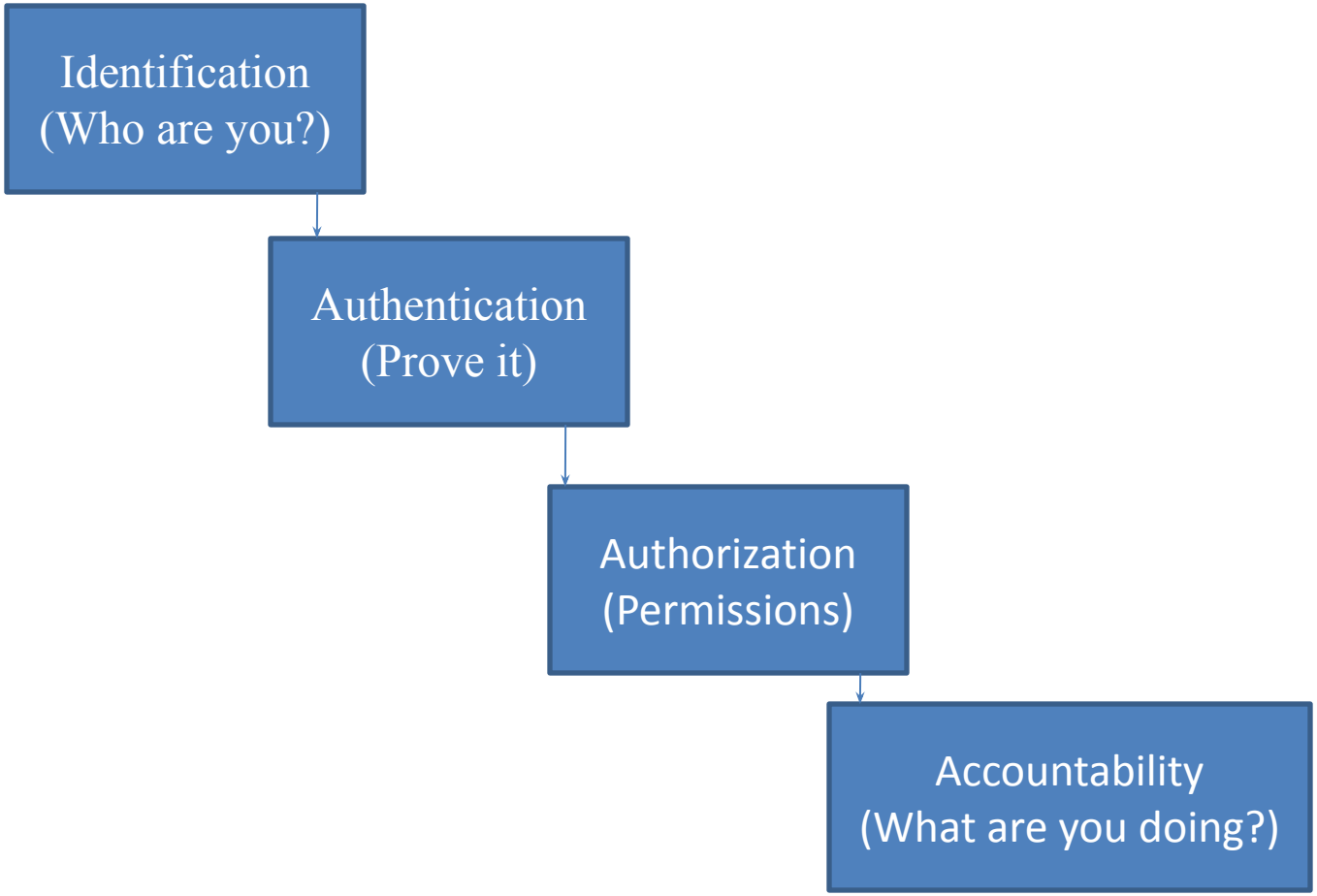
- **Control:**
  - Control is defined as policy , procedures, practices and organizational structures that are designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented or detected and corrected.
- **Objectives of control**
  - Authorization
  - Completeness
  - Accuracy
  - Validity
  - Physical safeguard and security
  - Error handling
  - Segregation of duties

Control of information system…

- **Categories of Controls**
  - Preventive - Avoid incident
  - Detective - Identify incident
  - Corrective - Remedy circumstance/mitigate damage and restore controls

Access control

Access control : Mechanism to protect the assets!



Access control…

Identification

- Method of establishing the subject's identity
  - User, Program, Process
- Use of username or other public information
- Identification component requirements:-
  - Each value should be unique
  - Follow a standard naming scheme
  - Non-descriptive of the user's position or tasks
  - Must not be shared between users

Authentication

- Method of proving the identity
- How to prove an identity?
  - Something you know
  - Something you have
  - Something you are
- Use of passwords, token, or biometrics other private information
- **What is two factor authentication?**
  - Strong authentication

Access control…

Authorization

- Method of proving the identity
- How to prove an identity?
  - Something you know
  - Something you have
  - Something you are

- Use of passwords, token, or biometrics other private information
- What is two factor authentication?
  - Strong authentication

Accountability

- Every individual who works with an information system should have specific responsibilities for information assurance.
- For example, the use of unique user identification and authentication supports accountability; the use of shared user IDs and passwords destroys accountability.

Access Control Models

Frameworks that dictate how subjects access objects

- Three Main Types
  - Discretionary Access Control (DAC)
  - Mandatory Access Control (MAC)
  - Role Based Access Control (RBAC)

- **Discretionary Access Control**
  - Allows the owner of the resource to specify which subjects can access which resources
  - Access control is at the discretion of the owner
  - DAC defines access control policy
    - That restricts access to files and other system resources based on identity
- **Mandatory Access Control**
  - Based on security label system
  - Users given security clearance and data is classified
  - Used where confidentiality is of utmost importance
  - MAC is considered a policy based control
  - Every object and subject is given a sensitivity label
    - Classification level
      - Secret, Top secret, Confidential, etc
    - Category
      - HR, Finance

Role Based Access Control

- Uses centrally administered set of controls to determine how subjects and objects interact
- Decisions based on the functions that a user is allowed to perform within an organization
- An advantage of role based access controls is the ease of administration

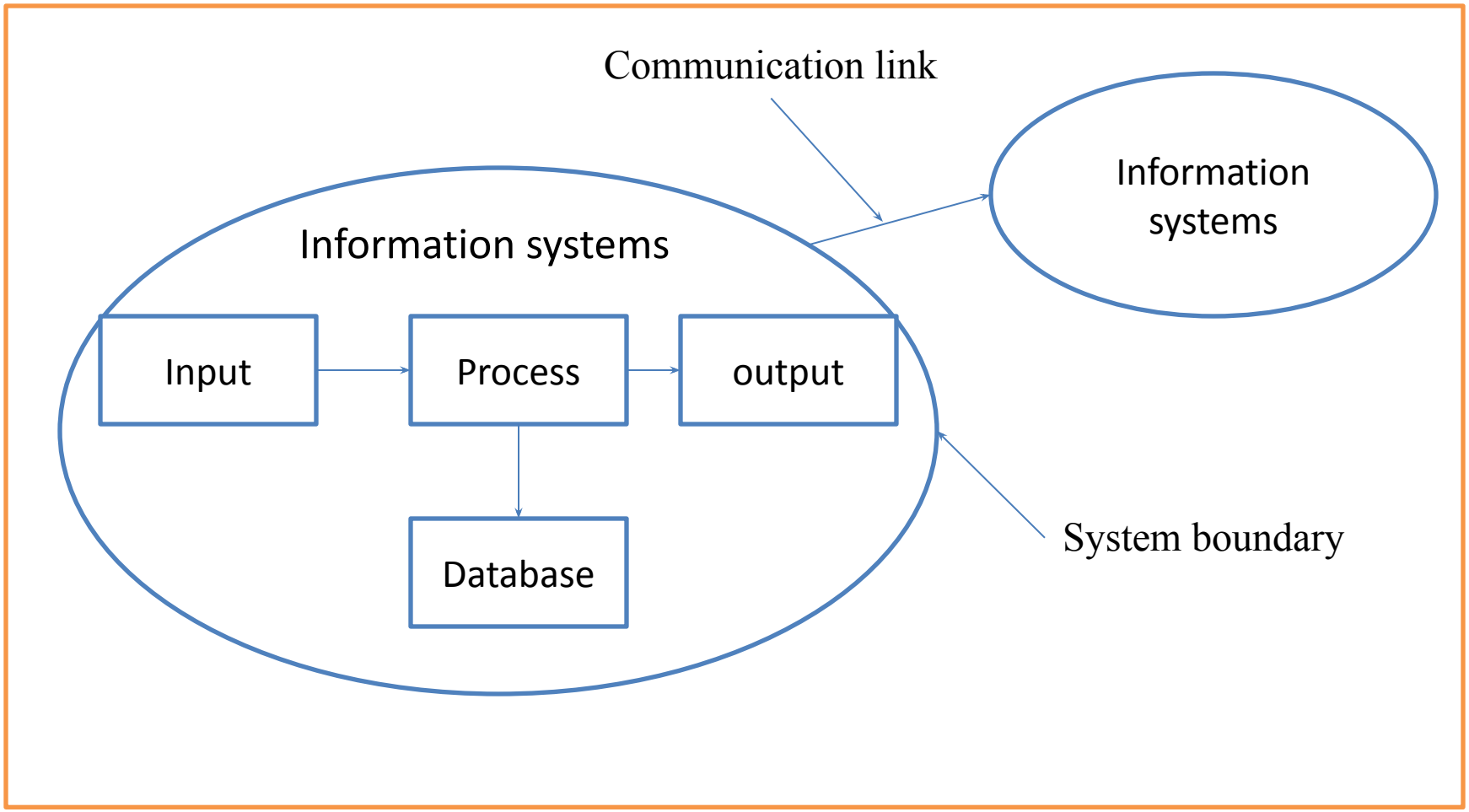
The principle of least privilege

- The principle of least privilege is a security strategy applicable to different areas, which is based on the idea of only granting those permissions that are necessary for the performance of a certain activity
- A good security practice

Information system controls

- Protection of information resources requires a well-designed set of controls.
- Computer systems are controlled by a combination of **general controls** and **application controls**
- **General controls**
  - General controls govern the design, security, and use of computer programs and the security of data files in general throughout the organization's information technology infrastructure.
  - On the whole, general controls apply to all computerized applications and consist of a combination of hardware, software, and manual procedures that create an overall control environment.
- Types of general controls
  - Software controls
  - Hardware controls
  - Computer operations controls
  - Data security controls
  - Implementation controls
  - Administrative controls

Applications controls



Applications controls…

- **Application controls**
  - Application controls include both automated and manual procedures that ensure that only authorized data are completely and accurately processed by that application.
  - Types of application controls
    - Boundary control
    - Input control
    - Processing control
    - Output controls
    - Database controls
    - Communication controls

Audit of information system

- Information audit is the process to discover, monitor, analyze and evaluate the information flow within an organization so as to implement, maintain and improve the organizational information management.
- An IT audit is the examination and evaluation of an organization's information technology infrastructure, policies and operations.
- Information technology audits determine whether IT controls protect corporate assets, ensure data integrity and are aligned with the business's overall goals.
- IT auditors examine not only physical security controls, but also overall business and financial controls that involve information technology systems.

Audit objective

- **Existence**: Verify that the assets , liabilities , ownership and /or activities are real
- **Authorization**: verify that the events have been occurred in accordance with management ‘s intend
- **Valuation**: Verify that the accounting values fairly present item worth.
- **Compliance**: verify that the processing is in compliance with the government laws and regulations.
- **Operational** : Verify the program , area or activity is performed economically , efficient and effectively
- **Risk management**
- **Integrity**

- **Implementation**: Assisting management to find out ways to implement internal control recommendation.
- **Participation**: Participating in specifying and designing computer controls and other features for systems to be installed.
- **Efficiency**: Determine whether efficient use is made of organizations computers resources.
- **Business objectives:** Determine whether computer system used accomplishes the business objectives and goal.
- **Improvement**
- **Adequate**

Audit process

Audit planning process

- **Understand the Business**
  - Identify the organization's strategies & business objectives
  - Understand the high risk profile for the organization
  - Identify how the organization structures their business operations
  - Understand the IT service support model
- **Defining the IT Audit area**
  - Examining the Business Model
  - Role of Supporting Technologies
  - Annual Business Plans
  - Centralized and Decentralized IT Functions
  - IT Support Processes
  - Define Audit Subject Areas
- **Perform Risk Assessment**
  - Develop processes to identify risks
  - Assess risk and rank audit subjects using IT risk factors

Audit planning process…

- **Formalize Audit Plan**
  - Select audit subjects and bundle into distinct audit engagements
  - Determine audit cycle and frequency
  - Add appropriate engagements based on management requests or opportunities for consulting
  - Validate the plan with business management

Assessment process

- On-site audit management,
- Meeting with the auditee, understanding the process and system controls and verifying that these controls work,
- Communicating among team members, and communicating with the auditee.

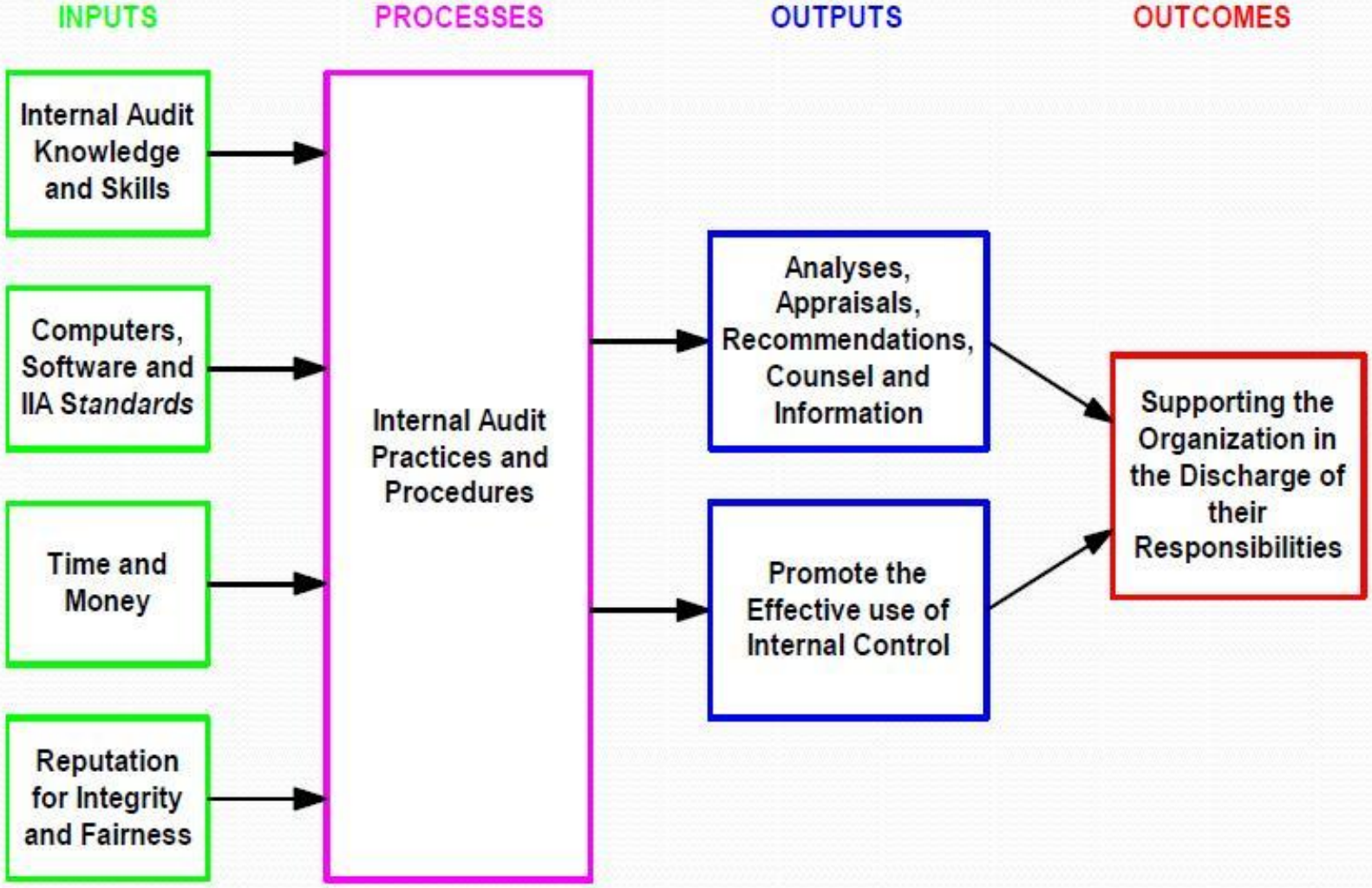
Reporting

- The purpose of the audit report is to communicate the results of the investigation.
- The report should provide correct and clear data that will be effective as a management aid in addressing important organizational issues.
- State the scope, objectives, period of coverage and the nature and extent of the audit work performed
- State the findings, conclusions, recommendations and any reservations or qualifications that the auditor has with respect to the audit

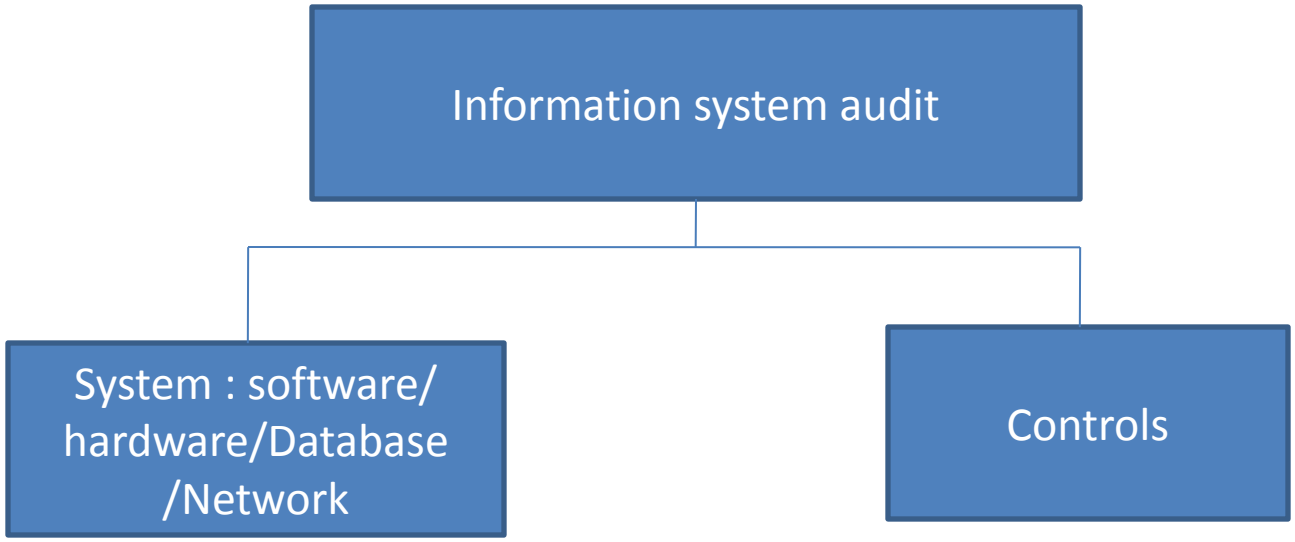
Follow-up

- The audit is completed when all the planned audit activities have been carried out, or otherwise agreed with the audit client.
- Reviewing the information technology audit report.
- Reviewing the management action plans related to the recommendations in the audit report.

The Audit Process Model

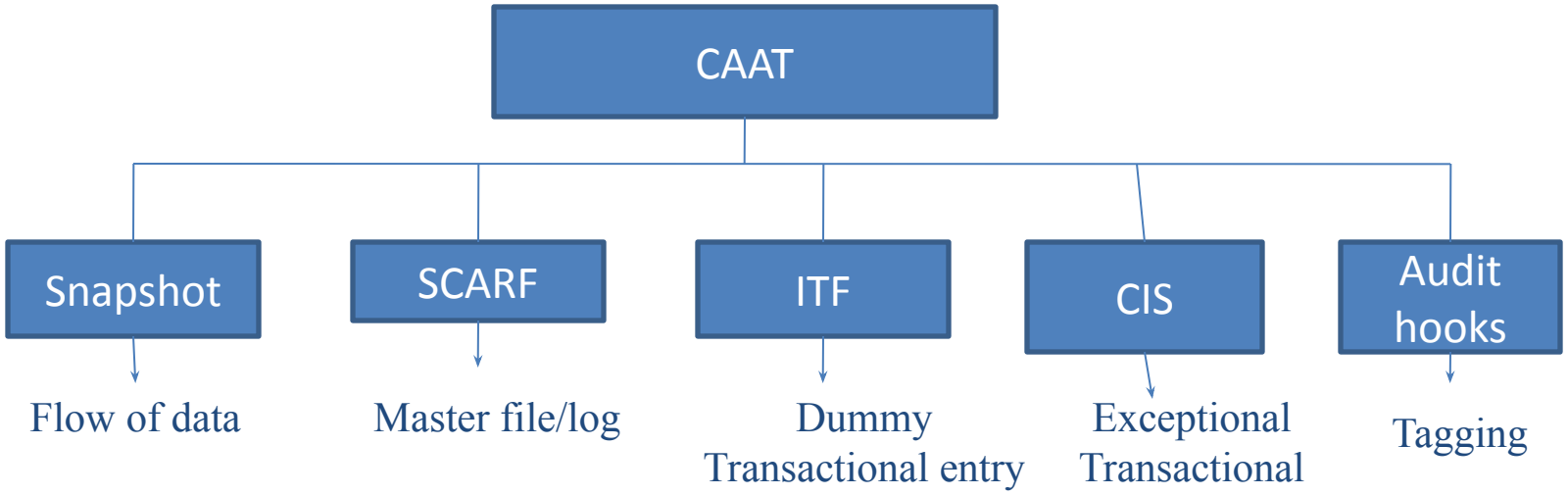


- In information system audit ,basically we perform system (software , hardware, database, network) and control audit.



Computer Assisted Audit Technique (CAAT)

- Also known as Computer Aided Audit Technique
- CAAT is the practice of using computers to automate the audit processes.



SCARF – System Control Audit Review File

ITF – Integrated Test facility

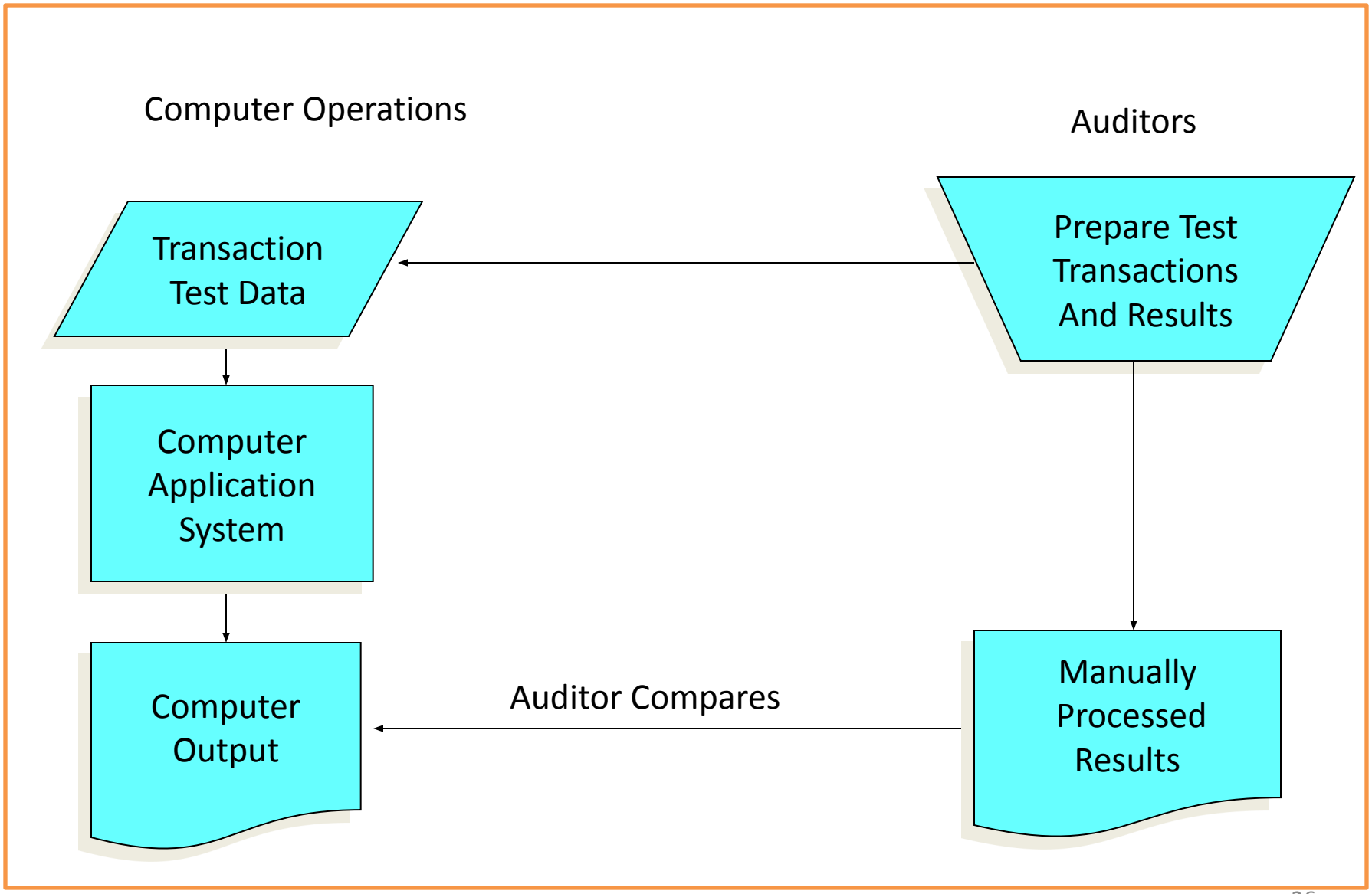
CIS- Continuous and Intermittent Simulation

- **Snapshot**
  - Snapshot help to trace any particular transaction in a computerized system.
  - Snapshot takes snap(i.e. image or picture) of the flow of transaction
  - These image can be used to verify authenticity , accuracy, and completeness of transaction processing
  - Main challenge in implementations of snapshots is to decide the location of snapshot points i.e. which images to be captured so that data can be captured in meaningful way.
- **SCARF (System control audit review file)**
  - Embedding audit software module within a host application system to provide continuous monitoring
  - Information collected is written into a special audit file- the SCARF master file
  - SCARF file records only those transactions which are of special audit significance such transactions above specified limit or transactions related to deviation/ exceptions.

- **Integrated Test Facility (ITF)**
  - A dummy ITF center is created for the auditors.
  - Auditors create transactions for controls they want to test.
  - Working papers are created to show expected results from manually processed information.
  - Auditor transactions are run with actual transactions.
  - Auditors compare ITF results to working papers
- **Continuous and Intermittent Simulation**
  - This technique can be used whenever the application system uses DBMS.
  - DBMS reads the transactions which is passed to CIS. If the transaction is as per selected criteria , the CIS examines the transaction for the correctness.
  - CIS determines whether any discrepancies exists between the result in produces and those the application system produces.

- **Audit hooks**
  - These are audit software that captures suspicious transactions
  - Criteria for suspicious transactions are designed by auditors as per their requirements
  - Helps the IS auditor to act before an error or an irregularity gets out of hand.
- **Test data**
  - The auditor prepares input containing both valid and invalid data.
  - Prior to processing the test data, the input is manually processed to determine what the output should look like.
  - The auditor then compares the computer-processed output with the manually processed results.

Illustration of Test Data Approach



Methodological Approach to Information Audit

1. Cost Benefit Method:
   - It lists information system options and compares them on the basis of their cost and perceived benefits.
2. Geographical Approach:
   - It identifies the components of information system and maps them in relation to one another to identify and meet system needs.
   - This is done by means of information resources mapping, i.e. mapping the information flows in the organization
3. Hybrid Approach:
   - It takes both geographical approach and cost benefit method into consideration.
   - It emphasizes on the control and management procedures for organizational strategy.
4. Management Information Audit:
   - It focuses on reports related to the management information.
5. Operational Information Audit:
   - It focuses on the efficiency and effectiveness with which information resources are used and accounted for.
   - It measures reliability of information system and compliance with obligations, regulations and standards.

Benefits of Information Audit

- It examines the information against the criteria under the identified purpose of the audit to meet the standard compliance.
- It determines the user information needs.
- It lists the information resources available within an organization.
- It identifies the costs and benefits of the information resources available.
- It provides information about the working structure of the information system of an organization.
- It produces report that recommends for the information handling problems.
- It helps organization to make use of information for strategic planning and implementations.
- It aids in decision making and support.
- It enables organization to be dynamic i.e. adapt to necessary changes.
- Information audit helps to identify problems like data redundancy, duplication, inconsistency and cost to store and utilize data and information.
- Information audit helps to identify hidden assets of an organization, skills and expertise of staffs, market for further expansion and so on that would expand organizational opportunities.

Problems in Information Audit

- Support of senior management is very crucial for information audit and in most cases such support is not provided.
- It is difficult to decide whether to use internal auditors or external consultants.
- It is very tedious task to collect and gather necessary information for auditing.
- The information audit time span depends up on the size of an organization.
- It is difficult to establish costs and value of information

Security of information system

- **Security**
  - The quality or state of being secure—to be free from danger
  - A successful organization should have multiple layers of security in place:
    - Physical security
      - To Protect physical items, object or areas
    - Personal security
      - To protect the individual or group of individuals who are authorized
    - Operations security
      - To protect the details of a particular operation or activities.
    - Communications security
      - To protect communication media, technology and content
    - Network security
      - To protect networking components, connections and contents
    - Information security
      - To protect information assets

- **Information security**
  - Information security is the protection of information and its critical elements , including the system and hardware that use , store, and transmit that information.
  - Necessary tools: policy, awareness, training, education, technology
  - C.I.A. triangle was standard based on confidentiality, integrity, and availability

- C.I.A. triangle now expanded into list of critical characteristics of information

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
  - Confidentiality
  - Integrity
  - Availability
  - Authorization
  - Authentication
  - Identification
  - Accountability

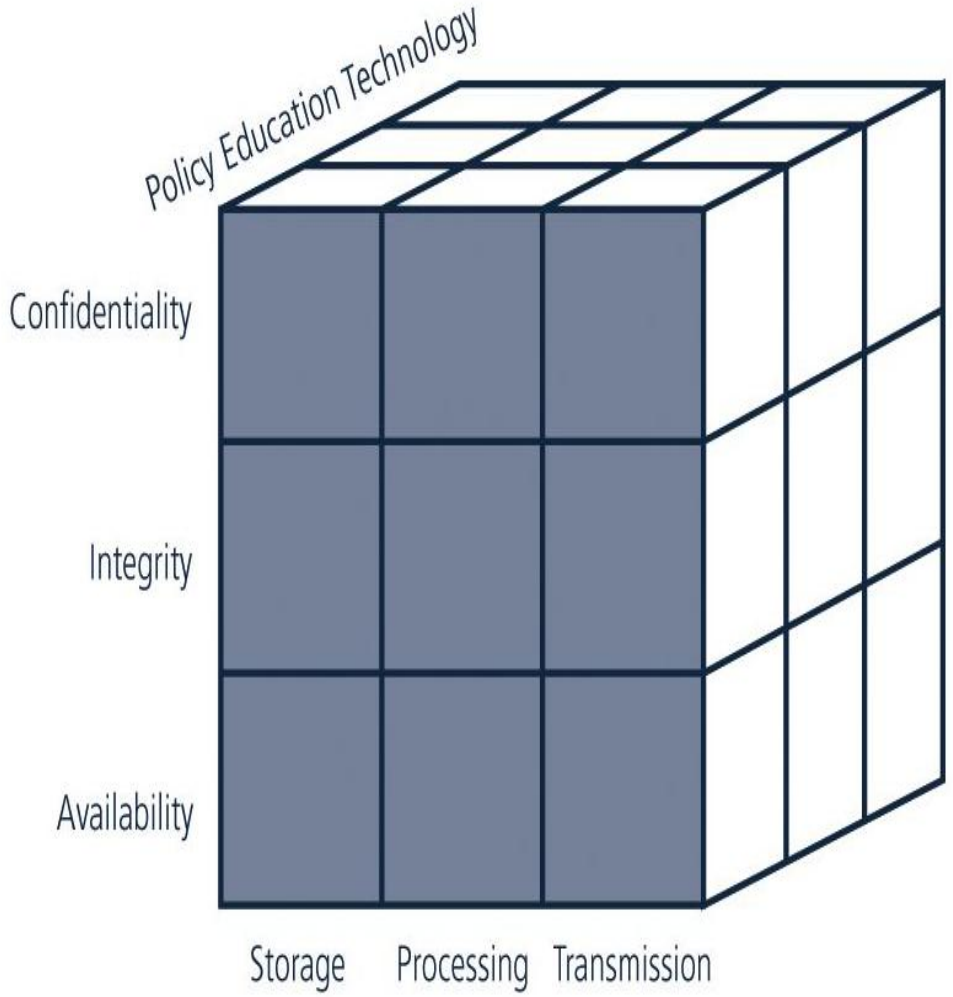
- **CONFIDENTIALITY(Secrecy/Privacy)**
  - When we talk about confidentiality of information, we are talking about protecting the information from disclosure to unauthorized parties.
  - Information has value, especially in today's world. Bank account statements, personal information, credit card numbers, trade secrets, government documents. Every one has information they wish to keep a secret. Protecting such information is a very major part of information security.
  - A very key component of protecting information confidentiality would be encryption. Encryption ensures that only the right people (people who knows the key) can read the information. Encryption is VERY widespread in today's environment and can be found in almost every major protocol in use.
  - A very prominent example will be SSL/TLS(secure Socket Layer/Transport Layer Security), a security protocol for communications over the internet that has been used in conjunction with a large number of internet protocols to ensure security.

- **Integrity (Truthfulness)**
  - Integrity means that data cannot be modified without authorization.
  - Integrity is the quality or state of being whole, complete, and uncorrupted.
  - The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being compiled, stored, or transmitted.
- **Availability(Accessible)**
  - Availability is the characteristic of information that enables user access to information without interference or obstruction and in a required format.
  - A user in this definition may be either a person or another computer system. Availability does not imply that the information is accessible to any user; rather, it means availability to authorized users.
  - For any information system to serve its purpose, the information must be available when it is needed.

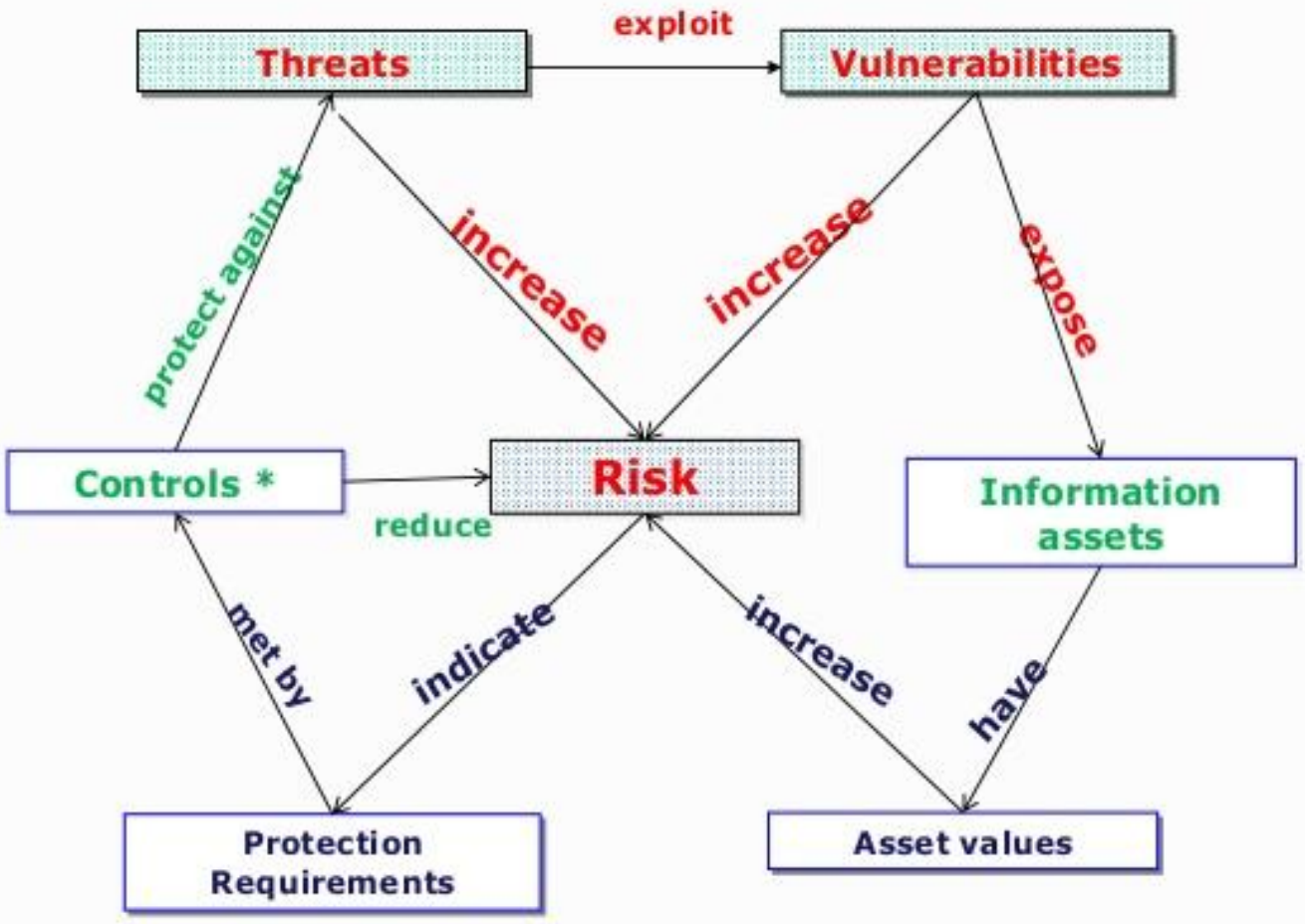
- **Authorization(Approval)**
  - Authorization to access information and other computing services begins with administrative policies and procedures. The policies prescribe what information and computing services can be accessed, by whom, and under what conditions, what actions they will be allowed to perform (run, view, create, delete, or change). The access control mechanisms are then configured to enforce these policies. This is called authorization.
  - To be effective, policies and other security controls must be enforceable and upheld. Effective policies ensure that people are held accountable for their actions. All failed and successful authentication attempts must be logged, and all access to information must leave some type of audit trail.
- **Authentication(Verification/Validation)**
  - Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.
  - Logically, authentication precedes authorization (although they may often seem to be combined). The two terms are often used synonymously but they are two different processes.
  - Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server.
  - If the credentials match, the process is completed and the user is granted authorization for access.

- **Identification(Recognition)**
  - Identification: It is how you identify someone, i.e., how you would call that person or company.
  - Could be the name, the account number in a bank, the username in some specific system.
- **Accountability(Answerability)**
  - The characteristic of accountability exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process.
  - For example, audit logs that track user activity on an information system provide accountability.

CNSS security model



Relationship between Risk, Threats, and Vulnerabilities



* Controls: A practice, procedure or mechanism that reduces risk

ISO 27001 security

- **Threat** can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.
- **Software attacks** means attack by Viruses, Worms, Trojan Horses etc.
- The various threats to information system are as follows:
  - DOS and DDOS Attack
  - Man-in-the middle attack
  - SQL Injection
  - Identity Theft
  - Social engineering
  - Phishing
  - Pharming
  - Malware
    - Virus
    - Worms
    - Trojan
    - Spyware
    - Ransomware

- **DOS and DDOS Attack**
  - A denial-of-service (**DoS**) is any type of **attack** where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a **DoS attack**, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses.
  - A distributed denial-of-service (DDoS) attack is a malicious attempt from many locations to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
- **Man-in-the middle attack**
  - A man-in-the-middle (MITM) attack is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized party.

- **SQL Injection**
  - SQL injection is a code injection technique that might destroy your database.
  - SQL injection is one of the most common web hacking techniques.
  - SQL injection is the placement of malicious code in SQL statements, via web page input.

- **Identity Theft**
- **Social engineering**
  - Social engineering is the art of manipulating people so they give up confidential information.
- **Phishing**
  - It is technique based on social engineering , Victim is asked to supply his/her personal information (ex: Fake Facebook Login page) usually through email or websites.
- **Pharming**
  - This Attack is usually redirecting your website traffic to a bogus website . This is done by changing host file or by exploiting on DNS server.

- **Malware** is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or a anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories:
  - Infection Methods
  - Malware Actions
- Malware on the **basis of Infection** Method are following:
  - **Virus**
    - They have the ability to replicate themselves by hooking them to the program on the host computer.
    - The Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.

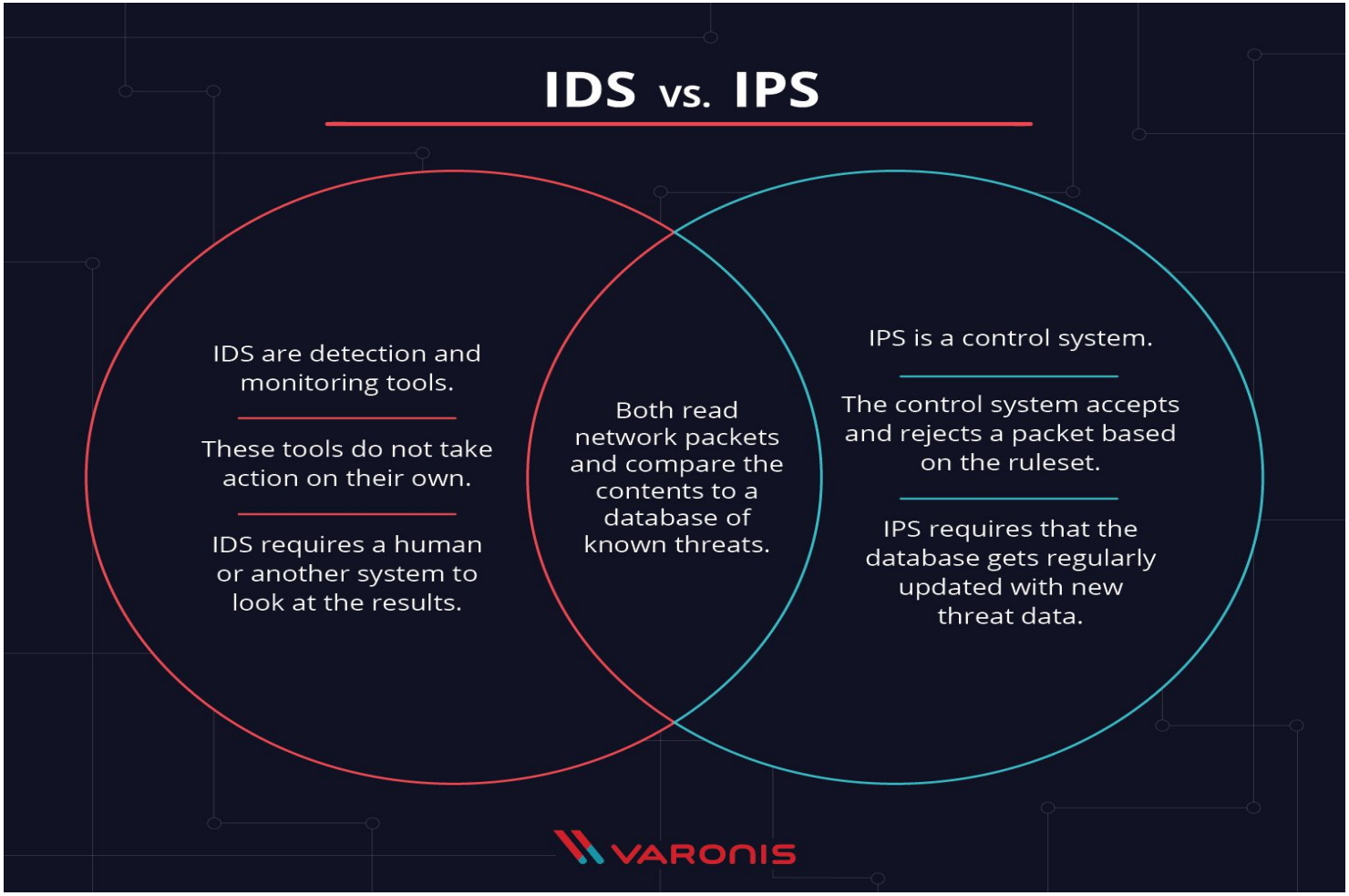
- Malware on the **basis of Infection** Method…
  - **Worms**
    - Worms are also self replicating in nature but they don't hook themselves to the program on host computer.
    - Biggest difference between virus and worms is that worms are network aware.
    - They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will for example consume hard disk space thus slowing down the computer.
  - **Trojan**
    - Trojans conceal themselves inside the software that seem legitimate and when that software is executed they will do their task of either stealing information or any other purpose for which they are designed.

- Malware on the **basis of Actions:**
  - **Spyware**
    - It is a program or we can say a software that monitors your activities on computer and reveal collected information to interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they installs themselves and sits silently to avoid detection.
    - One of the most common example of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.
  - **Ransomware**
    - It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money

Some Techniques That Will Help In Implementing These Security Mechanisms.

- Physical Access Security-protect network equipment such as servers, switches, and routers is to keep them in a locked, climate controlled, and fire protected environment
- Login / Password Security
- Anti-Virus Software
- Remote Access Security(a location not directly attached to the network.)
- Internet Firewalls
- Encryption
- Data Backups
- Disaster Recovery Plan
- Audits
- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)

- Intrusion detection systems (IDS) is the process of monitoring the events occurring in the network and analyzing them for signs of possible incidents, violations, or imminent threats to the security policies.
- Intrusion prevention systems (IPS) is the process of performing intrusion detection and then stopping the detected incidents.

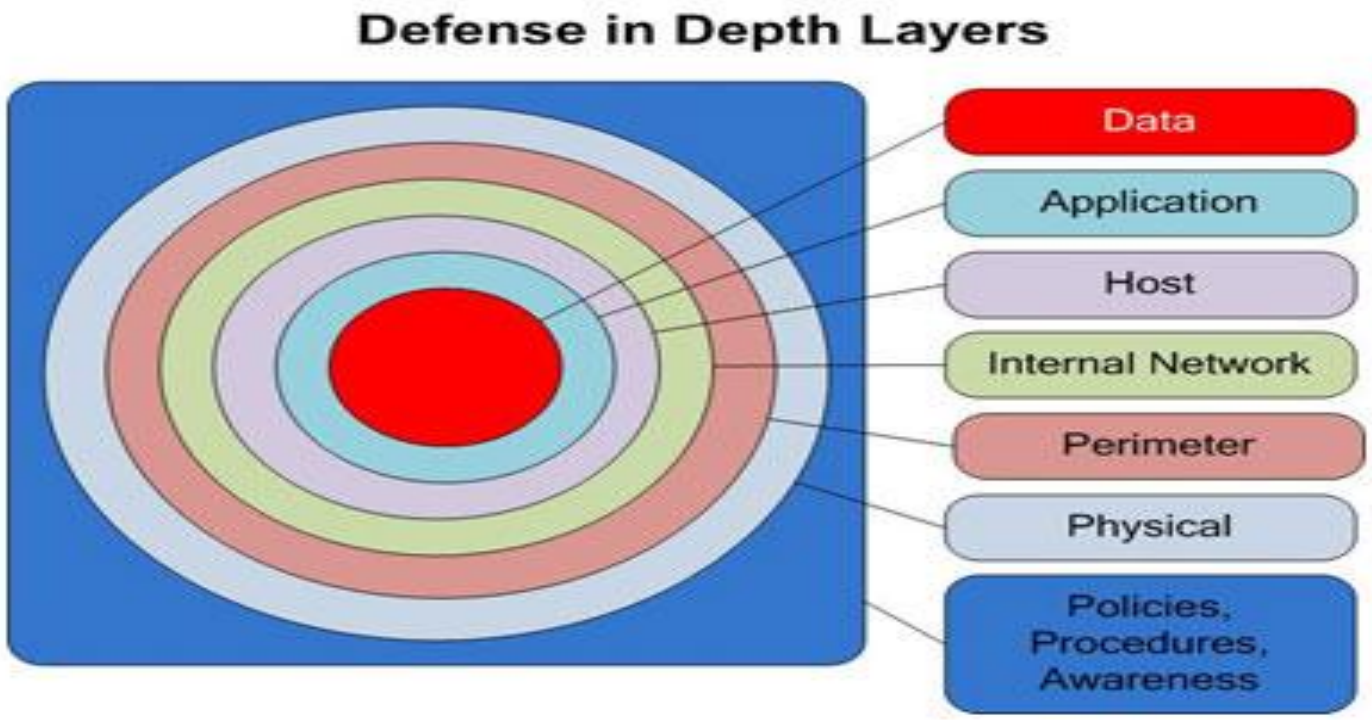


Organizational Security Models

- Some of the best practices that facilitate the implementation of security controls include :
  - Control Objectives for Information and Related Technology (COBIT),
  - ISO/IEC 17799/BS 7799,
  - Information Technology Infrastructure Library (ITIL),
  - Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE).
- Structure
  - Planning and Organization
  - Acquisition and Implementation
  - Delivery and Support
  - Monitoring

LAYERED SECURITY

- Also known as **defense in depth** makes use of multiple layers of defense to provide a robust security posture.
- Layered security, in its simplest form, consists of stacking security solutions, one on top of the other, to protect a computer from current, and **zero day** malware attacks



Why do we need it?

- To providing adequate computer system protection.
- Gaps exist in protection capabilities in even the most sophisticated security applications.

A CONSUMER LAYERED SECURITY APPROACH

- **Backup:** Consider where you would be if your layered security strategy failed. If you've ever lost critical data to a malware infection, no doubt you already consider it of primary importance.
- **Firewall** – is an application, or a hardware appliance, designed to block unauthorized access to your computer from the Internet, at the same time permitting authorized communications.
- **Antimalware** – A front line antimalware application is absolutely critical to avoid system infection.
- **Antivirus** – An antivirus application is another critical component in a layered defense strategy to ensure that if a malicious program is detected, it will be stopped dead in its tracks!
- **Web Browser Security** – Install a free Internet Browser add-on such as WOT(Web of Trust). WOT tests web sites you are visiting for spyware, spam, viruses, browser exploits, unreliable online shops, phishing, and online scams, helping you avoid unsafe web sites
- **Two factor authentication**
- **Single Sign on (SSO)**

Enterprise layered security strategy

- A modern enterprise security strategy uses a layered identity approach as the underpinning of its security.
- All enterprise systems, applications, information systems, facilities, buildings and rooms are assigned as enterprise risk.
- As the user digitally or physically approaches higher risk applications or a physical location the stronger authentication is used.
- As consider the enterprise firewall and the use of Id and passwords for login.

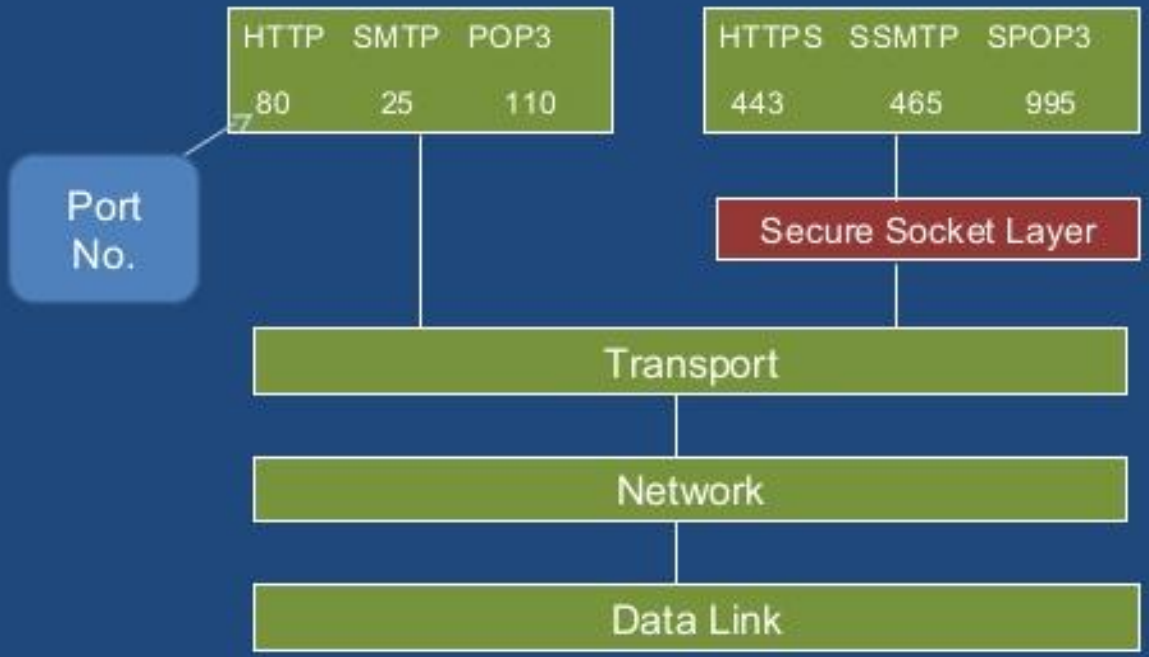
Implementing a Layered Identity Strategy: Enterprise Layered

- This could take the form of digital certificates, security tokens, smart cards and biometrics. It could also take the form of transactional security.
- While the user may successfully use their Id and password, the transaction security software would examine the IP address that the user is coming in from, their geographic position, the time of day, the type of physical computer the user is using and their behavioral pattern.
- If any of these differ from the past, then system alarm bells may start ringing resulting in the user being asked more personal questions, the action being stopped.

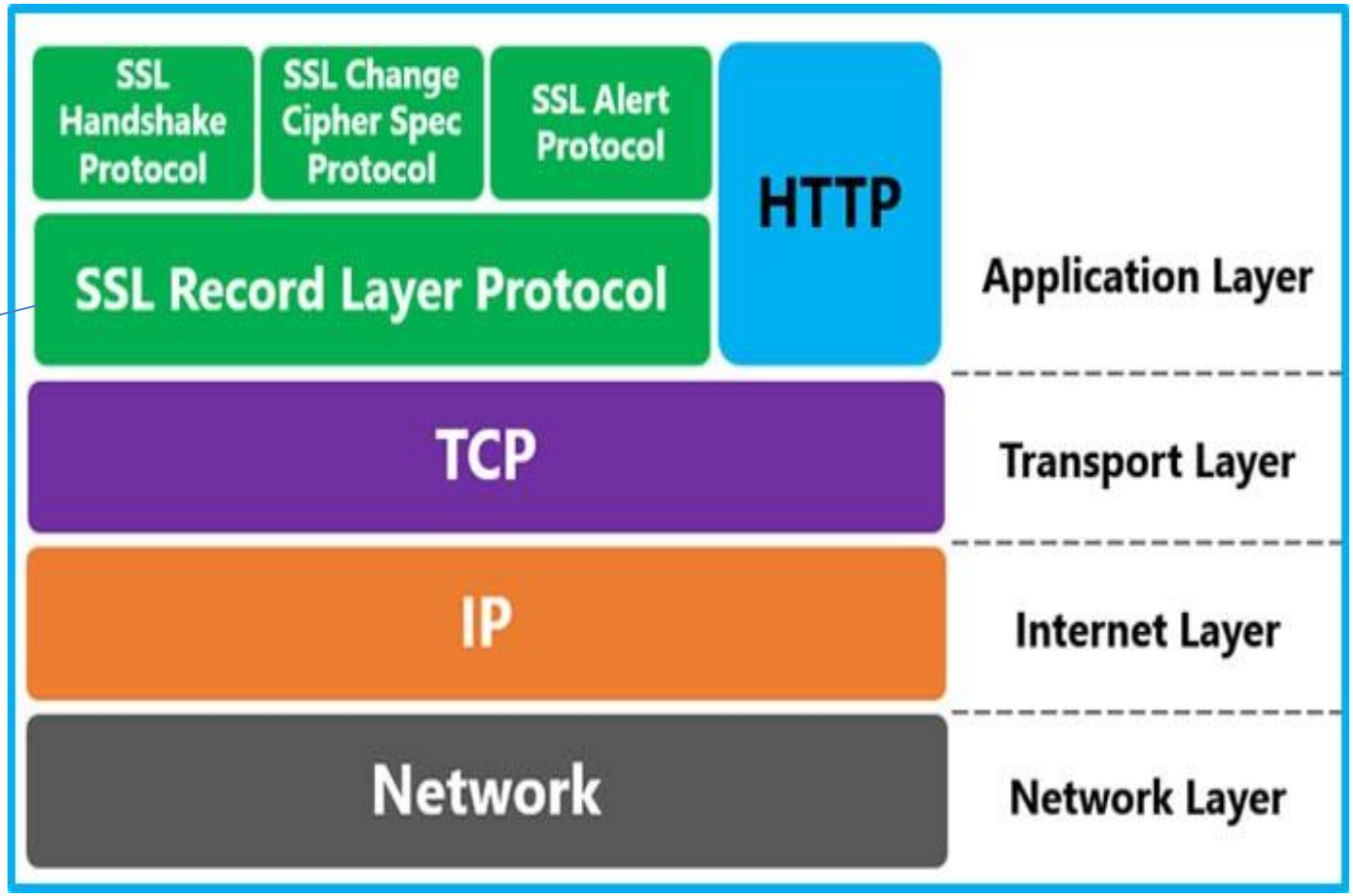
- **SSL**
  - Secure socket layer
  - Internet protocol for secure exchange of information between browser and server
  - Provides security in transport layer
- Goals
  - Confidentiality
  - Integrity
  - Authorization

Application	**HTTP, FTP,TELNET**
SSL	
Transport	TCP,UDP
IP	IP, ARP
Network layers	Ethernet

Where SSL fits?

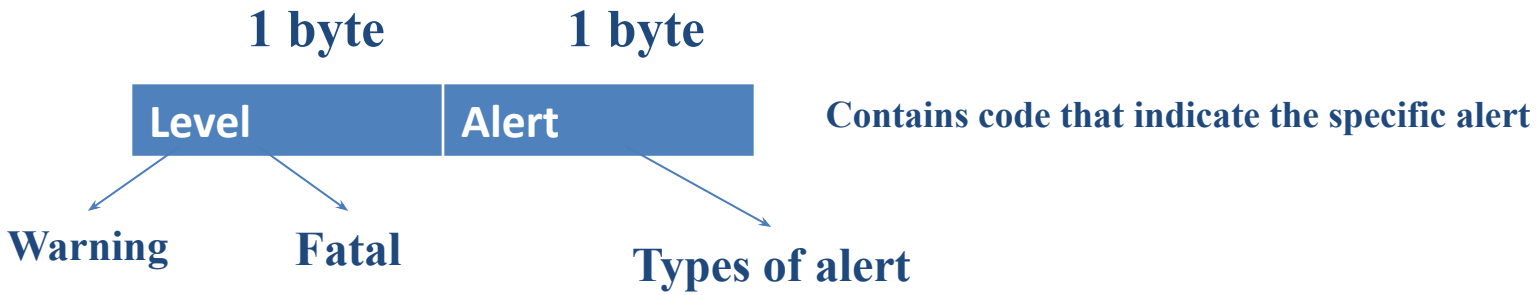


- **Working of SSL**
  - SSL protocol stack



- **SSL Record layer**
  - Provides two services for SSL connection
  - Confidentiality- Achieved by encryption
  - Message integrity – Achieved by Message Authentication Code (MAC)
- **SSL Change cipher Spec protocol**
  - Alert to a change in communication variables
  - The Change Cipher Spec Protocol is one of the three SSL-specific protocols that use the SSL Record Protocol, and it is the simplest.
  - This protocol consists of a single message , which consists of a single byte with the value 1.
  - The sole purpose of this message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.

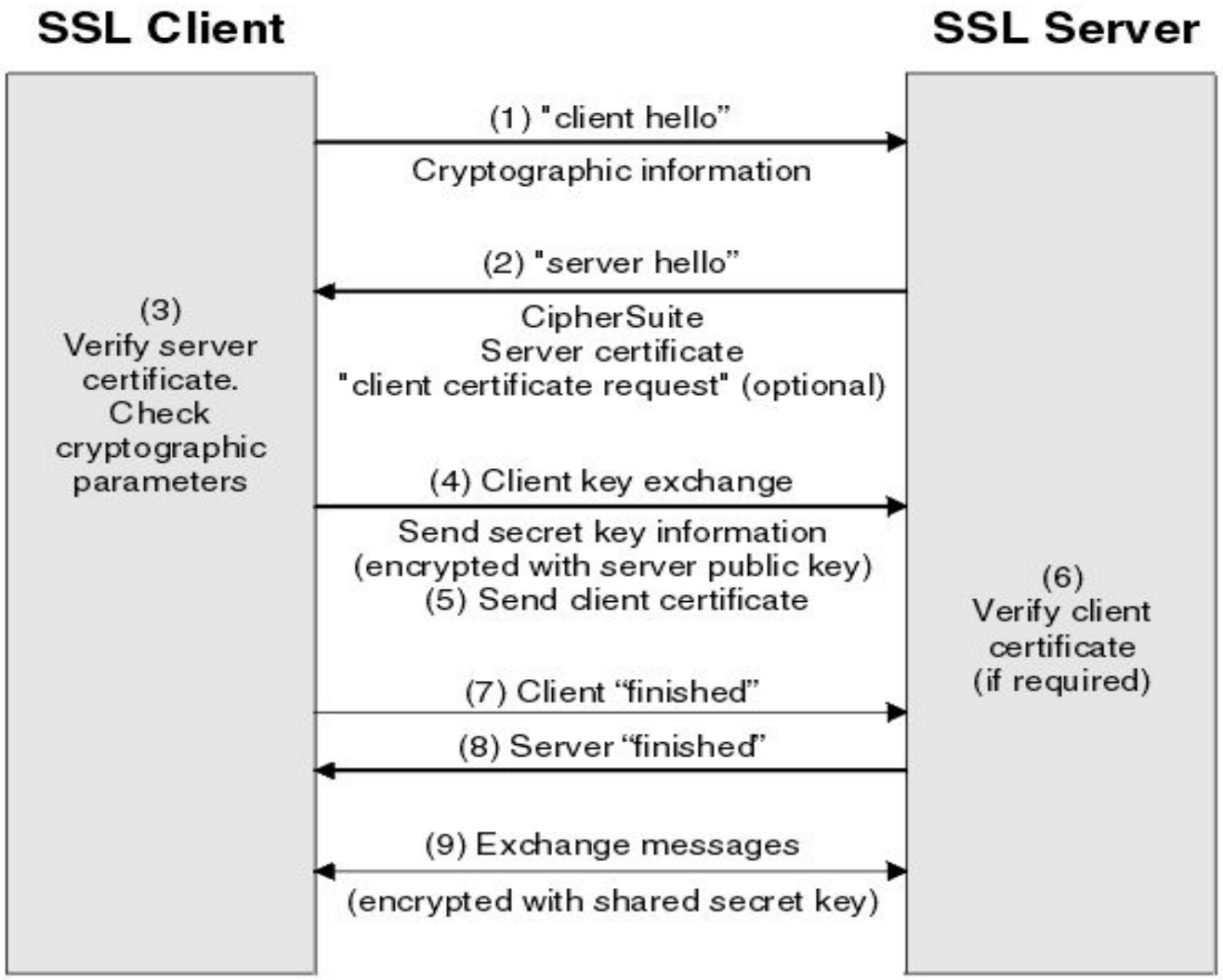
- **SSL Alert Protocol**
  - conveys SSL-related alerts to peer entity



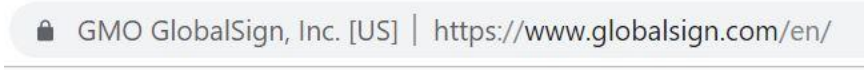
Alert message	Description
close_notify	Notifies the recipient that the sender will not send any more messages on this connection
unexpected_message	An inappropriate message was received.
bad_record_mac	An incorrect MAC was received.
bad_certificate	A received certificate was corrupt (e.g., contained a signature that did not verify).

- **SSL Handshake Protocol**
  - The most complex part of SSL.
  - allows server & client to:
    - authenticate each other
    - to negotiate encryption & MAC algorithms
    - to negotiate cryptographic keys to be used
  - comprises a series of messages in phases
    - Establish Security Capabilities
    - Server Authentication and Key Exchange
    - Client Authentication and Key Exchange

- **SSL Handshake Protocol**



- **Extended Validation:**
  - Extended validation is a certificate used for HTTPS websites and software that proves the legal entity controlling the websites or software package.
  - To obtain EV certificate, verification of the requesting entity's identity is required by a certificate authority.
  - It increases the security due to the identity validation process, which is indicated within the certificate by the policy identifier.
  - Website with EV SSL Certificate on Chrome shows padlock, HTTPS, organization name and office location country code.



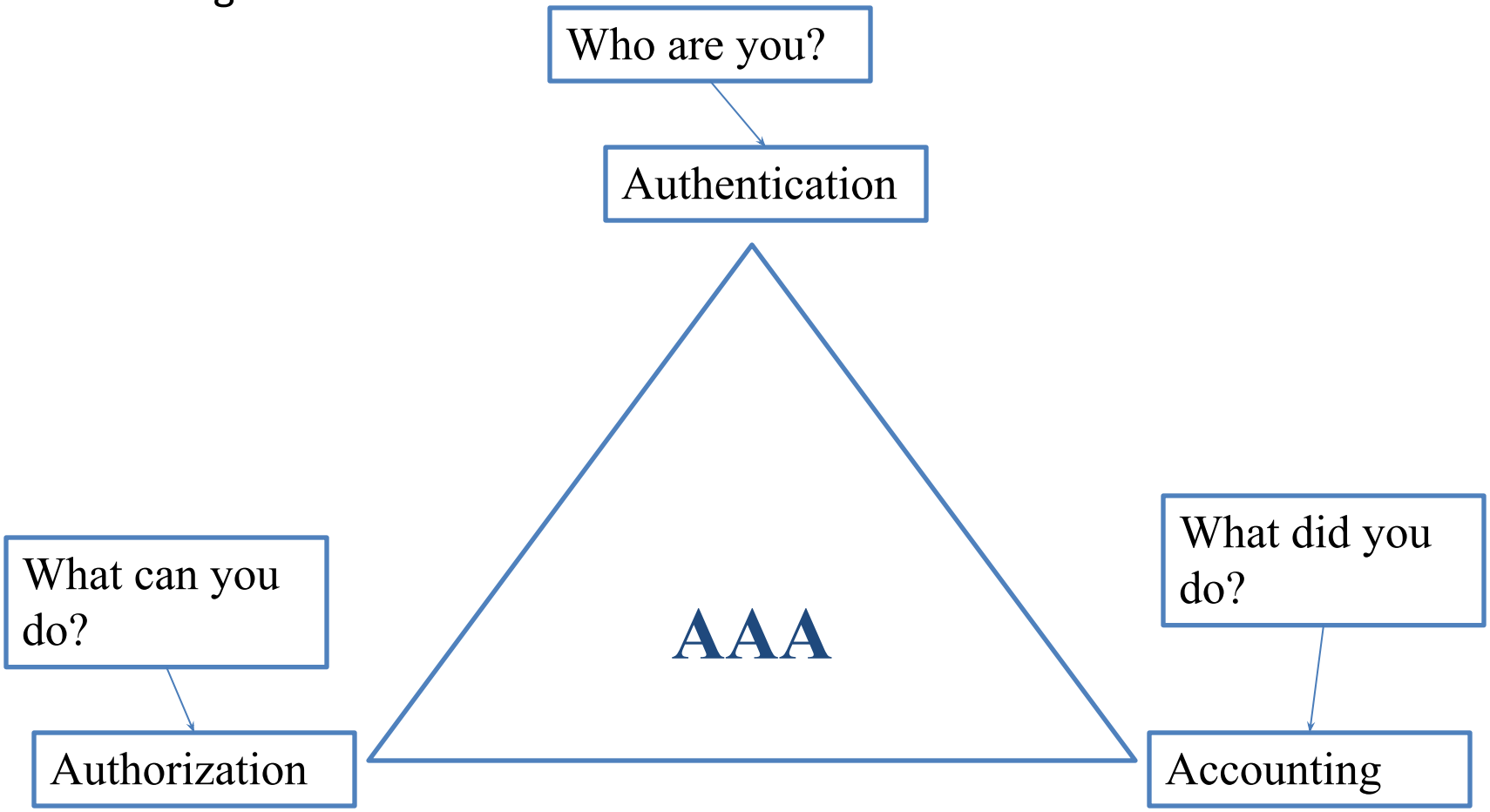
- **Remote access authentication**
  - Remote access authentication is the process by which a certified computer user can securely have network access and privileges even if the network is geographically separated.
  - It makes use of the digital certificate that contains information to identify the user to the server and provides the credentials.
  - The remote connection should be established to the network by the user as the network and the user computer are not physically connected to each other. Such remote connected is initiated by dial up connection or connection through Internet or connection through wireless medium.
  - Once the credentials within the digital certificate is verified by the server, the server provides access to the remote computer to access its resources and services.

Steps to obtain remote access authentication:

- Temporary network connection:
  - To initiate remote access to the server, the user computer must establish a temporary network connection to the server.
  - It may be through dial up, Internet or wireless connection.
  - The network connection is established securely using encryption for remote access protocols.
  - Proper encryption of communication channel is established to prevent from hijacking of authorized sessions and authorized user's credentials.
- Establishing proper privileges:
  - Once the network connection is successful, proper privileges to the requesting user should be established.
  - For this, three steps are performed namely authentication, authorization and accounting.
  - The server provides user identification to its user, computer or network device to enable remote access.

Steps to obtain remote access authentication…

- For this, three steps are performed namely authentication, authorization and accounting.



Telnet

- Telnet is the TCP/IP protocol standard that allows users to log on remotely and access resources as if the user had a local terminal connection to the server.
- The major threat of using Telnet is that it uses TCP/IP connection for information flow that has less security.
- The Telnet uses TCP port 23 for connection.

Secure Shell (SSH)

- SSH is a remote access system that provides a secure transport between machines using an SSH daemon at each end for secure login and secure file transfer.
- SSH provides higher level of security as it supports different encryption protocols, cryptographic host authentication and integrity protection.
- The authentication services are host based.

Content control / Content Filtering

- Content filtering is the process of controlling what content is permitted to the user.
- It is generally used to restrict material delivered over the Internet via Web, email or other means.
- It determines what content to make available or what content to block.

Implementation of content filtering

The content filtering can be implemented in various ways as follows:

1. Browser based filter:
   - It is implemented by using the third party browser extension.
   - On implementing such filters, the browser blocks the restricted content to be displayed to the users.
2. E-mail filter:
   - It is used to filter the information contained in the mail body or in the mail header.
   - The e-mail header or body or attachments are classified into accepted or rejected using the predefined rules or through artificial intelligence.
   - Only the accepted mails are shown to the users.
   - In most cases, the rejected messages are sent to the spam for manual review from the users.

Implementation of content filtering…

3. Client side filter:
   - It is generally installed on each client computer to allow content filtering.
   - Such filter can be managed, disabled or uninstalled by the user having administrative privileges on the system.
4. Content-limited ISP:
   - It includes the ISP that offer access to only a portion of Internet content.
   - Any users who pursue services from such ISP are subjected to restrictions.
5. Network based filtering:
   - It is implemented at transport layer (transport proxy) or application layer (web proxy).
   - It filters outbound as well as inbound information within a certain network.
   - All the clients of such network should accept the protocols and are subjected to restrictions.
6. Search engine filters:
   - Search engine itself provides the facility for safety filter.
   - When safety filter is activated, the inappropriate links that appears in the search lists are filtered out.
   - E.g. : https://www.kiddle.co

Policy-based encryption

- The Policy Based Encryption gateway automatically encrypts specific emails based on company-defined policies – that is, a set of rules designed to analyze all email, and encrypt any email that matches the pre-defined conditions.
- The concept of policy-based encryption is a promising paradigm for trust establishment and authorization in large-scale open environments like the Internet and Mobile Networks.
- On policy-based encryption which allow to encrypt a message according to a policy so that only entities fulfilling the policy are able to decrypt the message.
- More generally, policy-based encryption belongs to an emerging family of encryption schemes sharing the ability to integrate encryption with access control structures.
- A policy-based encryption scheme has to fulfill two primary requirements: on one hand, provable security under well defined attack models.
- On the other hand, efficiency, especially when dealing with the conjunctions and disjunctions of credential-based conditions.

Example of security in e-Commerce transaction

- **Electronic commerce**
  - Systems that support electronically executed business transactions
  - The fundamental purpose of e-commerce is to execute online transactions
- **Types of Ecommerce Models**
  - There are four main types of ecommerce models that can describe almost every transaction that takes place between consumers and businesses.
    - **Business to Consumer (B2C):**
      When a business sells a good or service to an individual consumer (e.g. You buy a pair of shoes from an online retailer).
    - **Business to Business (B2B):**
      When a business sells a good or service to another business (e.g. A business sells software-as-a-service for other businesses to use)

Types of Ecommerce Models…

- **Consumer to Consumer (C2C):**
  - When a consumer sells a good or service to another consumer (e.g. You sell your old furniture on eBay to another consumer).
- **Consumer to Business (C2B):**
  - When a consumer sells their own products or services to a business or organization (e.g. An influencer offers exposure to their online audience in exchange for a fee, or a photographer licenses their photo for a business to use).

- Transaction security is concerned with providing privacy in transactions to the buyers and sellers and protecting the client server network from breakdowns and third party attack. It basically deals with-
  - **Client security**- Techniques and practices that protect user privacy and integrity of the computer system.
  - **Server security** – Protect web server , software ,and associated hardware form breaks –ins, vandalism and DOS attacks
  - **Secure transaction**- Guarantee protection against eavesdropping and intentional message modification.

Security issues in e-commerce

- Malware
  - Virus
  - Worms
  - Trojan horse
- Unwanted programs:
  - Browser parasites- Programs used to monitors and change settings of user browser
  - Adware- Unwanted pop up ads
  - Spyware
- Phishing and identity theft
- Hacking
- Credit card fraud: It refers to use of stolen data to establish credit under false identity
- DOS , DDOS
- Insider jobs: It involves poorly designed server and client software and complexity of programs which increase vulnerabilities for hackers to exploit.

Defensive measures against security issues in E commerce

- Encryption
- Secure socket layer
- Secure hyper text transport protocol
- Trust Seal programs
- Digital signature

Thank you