Chapter 5 Access, Physical Control and Compliance Standards

Access

Access is the ability of subject to communicate with an object. Access control is the ability to specify, to control and to limit the access. Access control is to decide who can access what.

1) Identification:

1) It is most commonly used in access controls to check the identity of user of an information system.
2) Typical identification can be user name, email address, ID etc.

Q 1) Define Authorization and Authentication? Explain different methods used for authentication.

2) Authentication

Authentication is the process of determining the identity of a user or other entity. User authentication is performed during the log on process when user submits a username and password.

Generally there are three methods used in authentication.

(a) Something you know:

The most common authentication mechanism is to provide a user ID and password.

(b) Something you have: This method involves the use of something that only valid users should have like lock and key. Only those individuals with the correct key can be able to open the key.

(c) Something about you: This method involves something that is unique about you likr finger Print, Retina etc.

3) Authorization:

- Authorization is a process of verifying that a known person has the authority to perform a certain operation.
- Authorization takes place after identification and authentication of individual.

Access Control: - Access Controls use the mechanism to identify individuals who are attempting to enter a facility, area or system. From the security audit perspective, facility access control is an element that gets stringently verified.

Biometrics Access Control:

Biometrics refers to metrics related to human characteristics and traits. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control.

Q. 2) What is Biometric? List different types of biometrics used for authentication

Biometrics

Definition:

"Automated measurement of Physiological and/or behavioral characteristics to determine or authenticate identity.

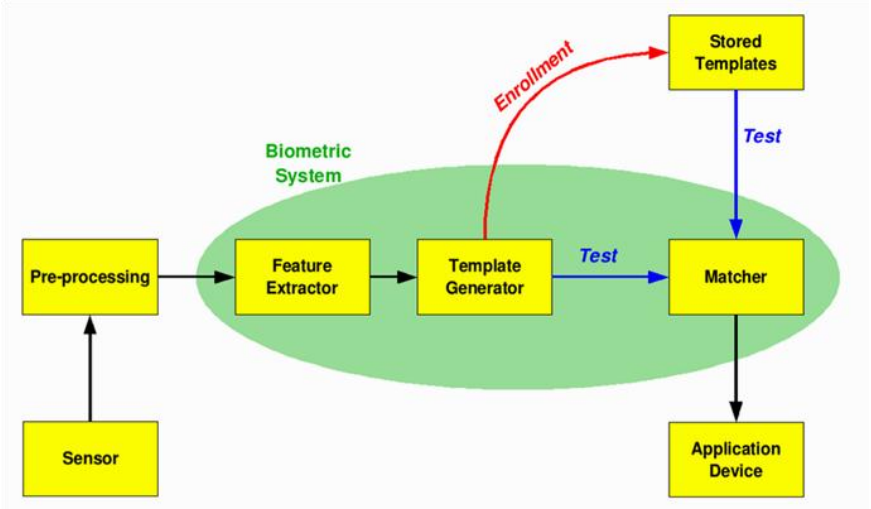
The term "Automated measurement" means No human involvement is there and the comparison takes place in Real-Time.

"Physiological and/or behavioral characteristics "consists of

1. Behavioral: It includes the way user speaks, types on a keyboard and signs the name.

2. Physiological: It includes the
   - Fingerprint
   - Hand
   - Eyes and
   - Face

- Benefits of Biometrics are:
  - Security
    - PC, Network, Web
    - Physical access to Buildings/Rooms
  - Accountability
    - Audit Trails
    - Recordkeeping
  - Convenience
  - Savings
- List of Biometrics used are
  - Handprint
  - Fingerprint
  - Retina
  - Voice/Speech
  - Handwriting/Signature
  - Face
  - Movement patterns (i.e typing Keystrokes etc)



Q 3) What is SSO? Explain its components.

Single Sign-On

- Single sign-on is a user/session authentication process that permits a user to enter one name and password in order to access multiple applications.
- The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

Advantages

- Reduced operational cost
- Reduced time to access data, e.g. ER
- Improved user experience, no password lists to carry

- Ease burden on developers
- Centralized management of users, roles

Disadvantages

Single Point of failure:

All systems go down if the SSO authentication server fails.

Single Sign-On has two components

1) Login Server :

The first time that a user want access to an application

- Login Server authenticates the user with the help of user name and password
- It passes the client's identity to the various applications.
- It marks the client being authenticated with an encrypted login cookie.
- In subsequent user logins, this login cookie provides the Login Server with the user's identity and indicates that authentication has already been performed.

2) SSO Application Programming Interface (API)

The Single Sign On API enables

- Applications to communicate with the Login Server and to accept a user's identity as validated by the Login Server.
- Administrators manage the applications association to the Login Server

Types of SSO Applications

- Partner Applications: Partner Applications are integrated with the Login Server. They contain a SSO API that enables them to accept a user's identity as validated by the Login Server.

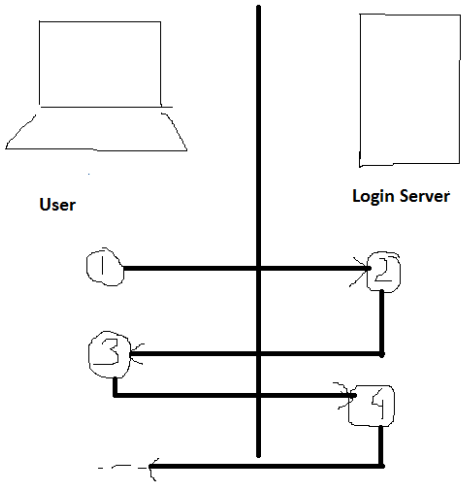
External Applications: External applications are web-based applications that retain their authentication logic. They do not delegate authentication to the Login server and as such require username and password to provide access

Q 4) Explain the working of SSO

Working of SSO

- Whenever a user accesses an application, the Login Server first authenticates that user.

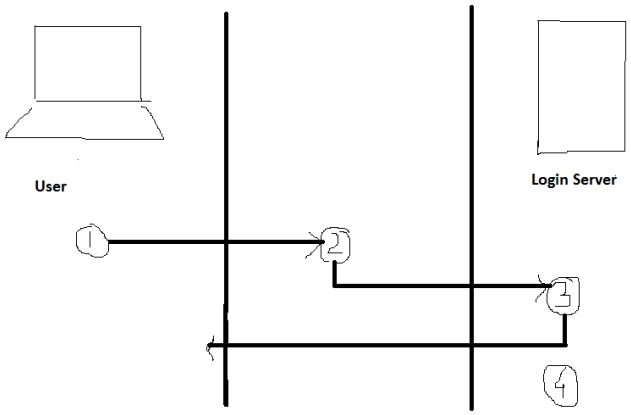
Authenticating to the Login Server



1) Login Server checks for login cookies. If one is present, the login server identifies the user from the encrypted information in the login cookie.
2) If a login cookie is not present, the login server prompts the user for the user's credentials
3) The user provide user name and password
4) The Login Server authenticates the user by passing the provided name and password to the configured authentication routine.

If authentication is successful, the Login Server establishes a Login Cookie on the client browser to facilitate SSO for future authentication requests.

Accessing a Partner Application



1) The user seeks the access to the partner application directly.
2) For the first time during a session, the user is accessing partner application, and then the partner application transparently directs the user to the Login Server to obtain authentication credentials.

3) The Login Server authenticates the user as describe in "Authenticating to the Login Server"

4) The Login Server transparently directs the user to the partner application. It does this by using a URL with an encrypted parameter containing the user's identity.

5) The Partner Application then decrypts the parameter, identifies the user, and establishes its own session management.

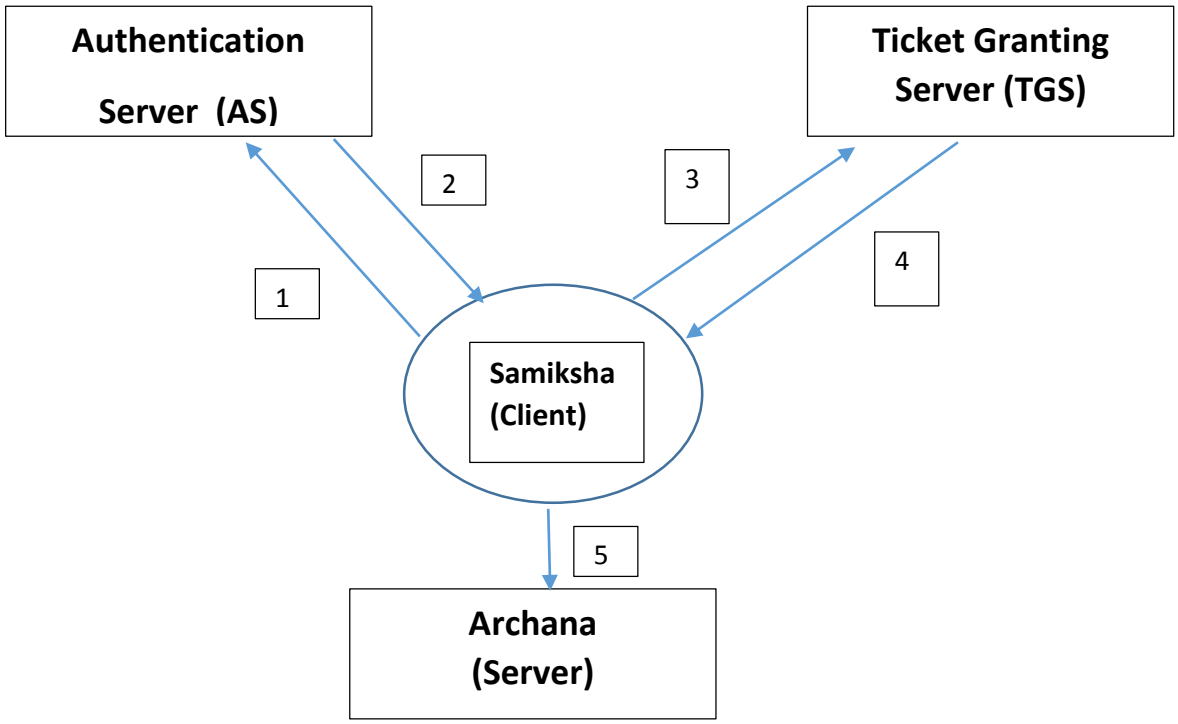
Q 5) Explain the working of Kerberos with diagram

KERBEROS

- Kerberos is a network authentication protocol and it is designed to provide strong authentication for Client /Server Applications. It uses secret- key Cryptography.
- Kerberos is a protocol which was created by MIT as a solution to network security problems. It uses strong cryptography hence a client can prove its identity to a server and vice versa over an insecure network connection.

Basics of Kerberos

- The basic Kerberos Model has the following participants:
- A Client
- A Server
- An Authentication Server (AS)
- A Ticket granting Server (TGS)



Suppose client (Samiksha) wants to communicate with server (Archana)
Using Kerberos protocol, Archana will verify the identity of samiksha and a session key will be established between Samiksha and Archana.

1. The Client (Samiksha) requests a ticket for ticket granting service from the authentication server. The authentication server has a strong database of password information for the entire clients.
2. AS returns an encrypted ticket i.e encrypted using Smaiksha's secret password information
3. Samiksha wants to use the service that Archana (Server) provides. So Samiksha submits her ticket to the ticket granting server.
4. The ticket granting server verifies the ticket for identifying Samiksha and after verification gives a new ticket to Samiksha that will allow her to make use of Archana's Service.
5. Samiksha now has a service ticket which she can submit to Archana. She sends Archana the service ticket as well as authentication credential. Archana checks the ticket with the authentication credential to make sure whether it is a valid client or not. After verification, Archana will provide the service to Samiksha (the client).

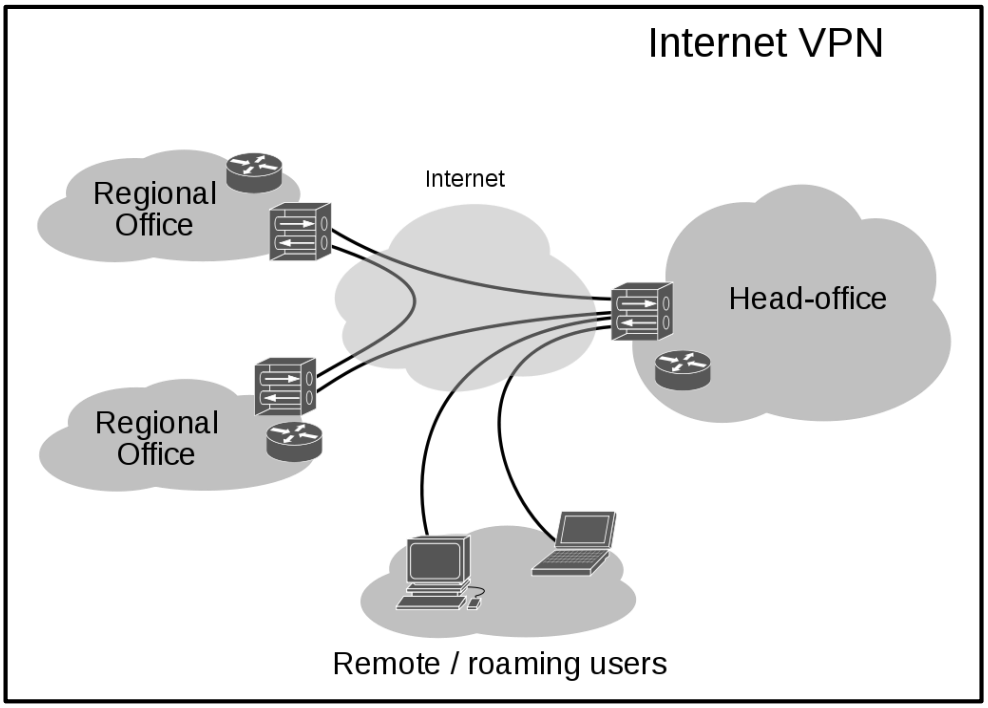
Q 6) List different methods used for remote user access and authentication. Explain any one in detail

Remote User Access and Authentication

Q 7) Explain VPN with neat diagram

1. Virtual Private Network (VPN)
   - VPN is a mechanism of employing encryption, authentication and integrity protection so that we can use a public network (the Internet) as Information Technology it is a private network.

- VPN offers high amount of security and yet does not require any special cabling on behalf of the organization that wants to use it. Thus VPN combines the advantages of public network (cheap and easily available) with those of a private network (secure and reliable)
- Suppose an organization has two networks, Network 1 and Network 2 which are physically apart from each other and we want to connect them using the VPN approach. In such case we set up two firewalls, Firewall1 and Firewall2



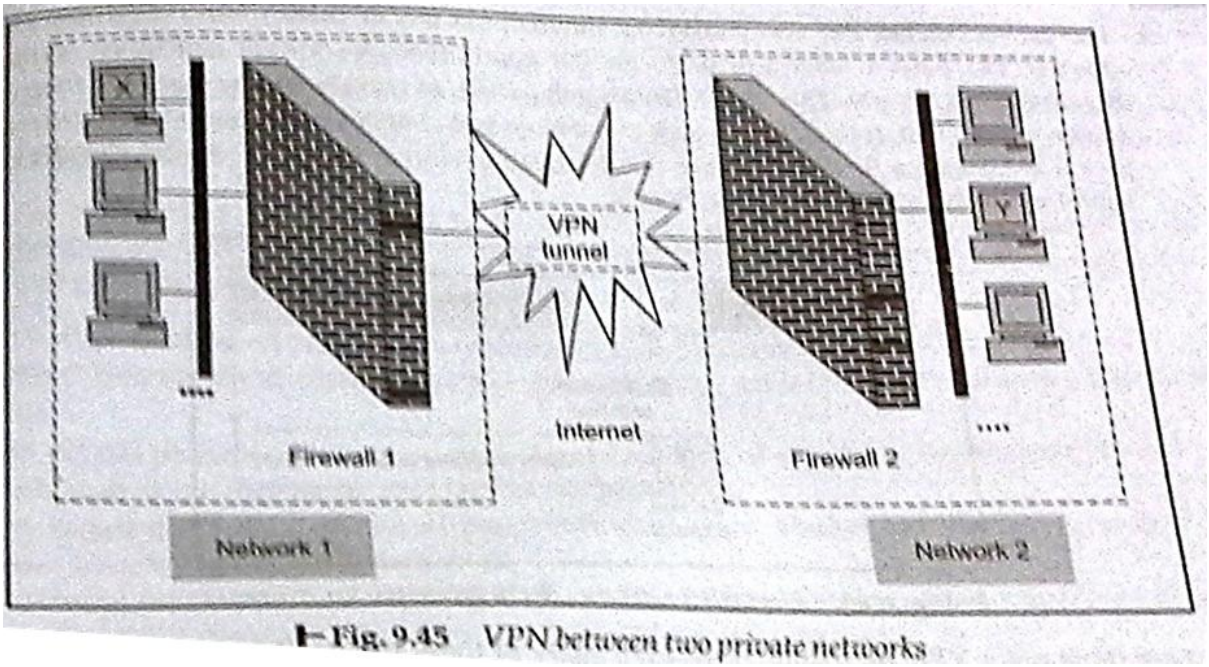
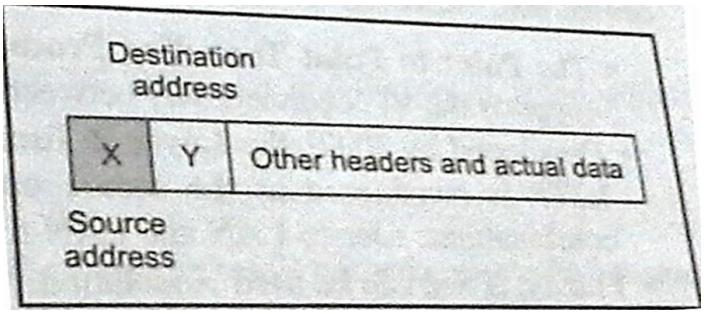


Fig. 9.45 VPN between two private networks

- Let us assume that host X on Network 1 wants to send a data packet to host Y on Network 2. This transmission would work as follows:

1) Host X creates the packet, inserts its own IP address as the source address and the IP address of host Y as the destination address.

Step 1: Original Packet



2) The packet reaches Firewall 1. As we know, Firewall1 now adds new headers to the packet. In these new headers it changes the source IP address of the packet from that of host X to its own address (i.e. the IP address of Firewall1 say F1). It also changes the destination IP address of the packet from that of host Y to the IP address of Firewall say F2) .It also performs the packet encryption and authentication depending on the settings and send the modified packet over the Internet.

Step 2 Firewall 1 changes the packet contents

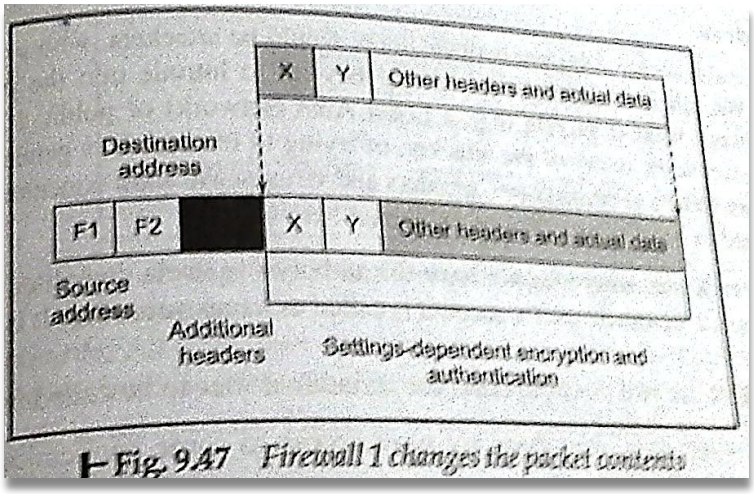
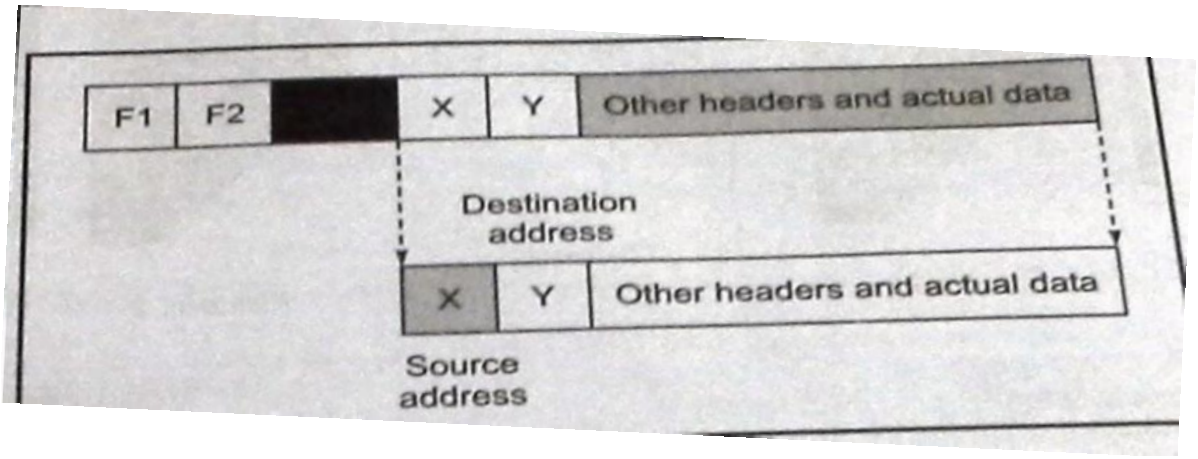


Fig. 9.47 *Firewall 1 changes the packet contents*

3) The packet reaches Firewall2 over the Internet via one or more routers. Firewall2 discards the outer header and perfomrs the appropriate decryption and other cryptographic functions as necessary. This yields the original packet as was created by host X in step 1. It looks for the destination and delivers the packet to host Y.

Step 3: Firewall 2 retrieves the original packet contents



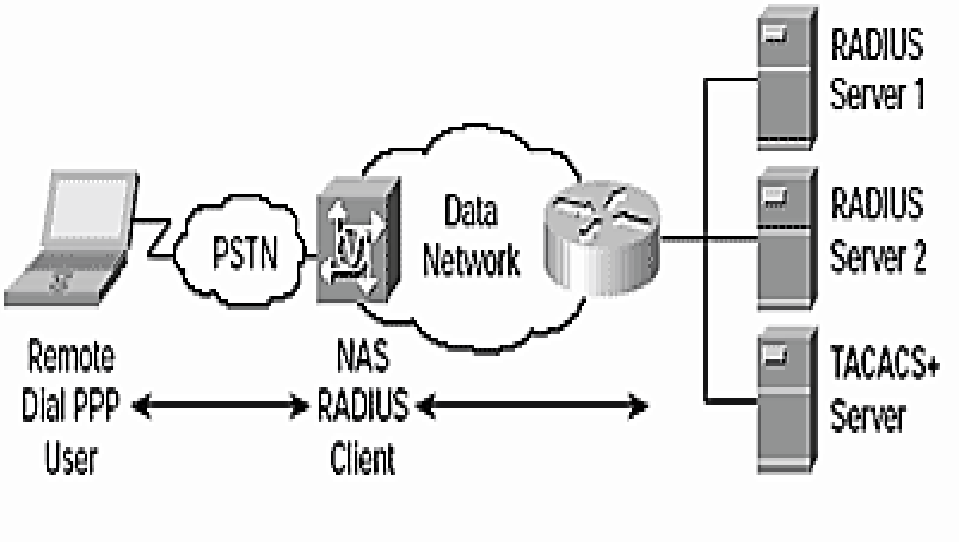
There are three main VPN protocols.

1) PPTP (Point to Point Tunneling Protocol)
   It is used on Windows NT Systems. It mainly supports the VPN connectivity between a single user and a LAN.
2) L2TP (Layer 2 Tunneling Protocol)
   L2TP is considered as the secure open standard for VPN connections. It works for both combinations: user to LAN and Lan-to-Lan.
3) IPSEC
   This is used between two communicating devices.

2. RADIUS (Remote Authentication Dial In User Service (RADIUS))

1. RADIUS is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server.
2. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport.
3. The Remote Access Server, the Virtual Private Network server, the Network switch with port-based authentication, and the Network Access Server (NAS), are all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server

   Simple RADIUS Network Diagram



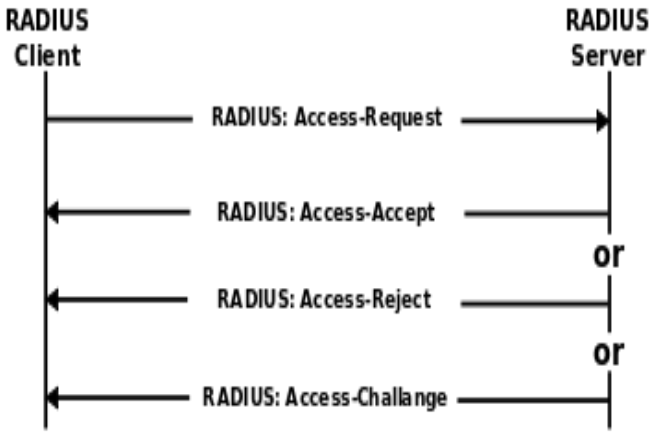
Features of RADIUS

- Client/Server Model:
  - NAS will work as a client for RADIUS server.
  - RADIUS server is responsible for getting user connection requests, authenticating the user and then returning all configuration information necessary for the client to deliver service to the user.
  - A RADIUS server can act as a proxy client to other RADIUS servers.
- Network Security:
  - Transactions between client and server are authenticated through the use of a shared key and this key is never sent over the network.
  - Password is encrypted before sending it over network.
- Flexible Authentication Mechanisms:
- RADIUS supports following protocols for authentication purpose:
  - Point-to-Point Protocol - PPP
  - Password authentication protocol - PAP
  - Challenge-handshake authentication protocol - CHAP
  - Simple UNIX Login

Operations of RADIUS

- Before Client starts communicating with RADIUS Server, it is required that shared secret must be shared between Client and Server and Client must be configured to use RADIUS server to get service.
- Once Client is configured properly then :
- Client starts with Access-Request.
  - Server sends either Access-Accept, Access-Reject or Access-Challenge.
  - Access-Accept keeps all required attribute to provide a service to user

RADIUS Authentication and Authorization Flow



PHYSICAL CONTROL

- Physical Access Control

Q 9) Explain different physical security controls (Write the details)

- Physical Security Controls:
  - Walls, Fencing and Gates
  - Guards (Patrol force/ Security Guard)
  - Dogs
  - ID Cards and Badges
  - Locks and Key
  - Electronic Monitoring
  - Alarms and Alarm System
  - Computer room and Writing Closets
  - Interior Wall and Doors
- Physical Access Threats

Q 10) Explain major sources of physical security threats (Write the details)

- Physical Security Threats:
  - Weather
  - Fire and Chemical
  - Earth Movement
  - Object Movement (Structural failure) building collapse, falling truck, plane, car
  - Energy (electricity, magnetism, radio wave etc.)
  - Organism (Biological): Virus, bacteria, animal etc.
  - Equipment: Mechanical/electronic component failure
  - Human: Strike, War, Sabotage etc.

Q 11) List various methods to provide physical security?

Providing Physical Security

1. Educating People

Q 12) Explain Administrative access control in detail.

2. Administrative Access Controls
   a) Restricting Work Areas
   b) Escort requirements and Visitor Control
   c) Site Selection while planning facility : Following points should be considered for site selection - Visibility, Local considerations, Natural disasters, Transportation, Physical Security Controls (Perimeter Security Controls,

badge, Keys and combination Locks, Security Dogs, Lighting- motion detector lights, floodlights, streetlights or searchlights etc.

3. Technical controls
   - Smart Cards,
   - Audit Trails,
   - Intrusion Detection/ Alarm Systems,
   - Biometric Access controls,
   - Environmental/ Life Safety Controls
     - Power,
     - Fire Detection,
     - Heating, Ventilation and Air Conditioning (HVAC)

Compliance Standards

1. Implementing and Information Security Management System (ISMS)
2. ISO 27001
3. ISO 20000
4. BS 25999 (British Standard)
5. PCI DSS (Payment Card Industry Data Security Standard)
6. ITIL Framework
7. COBIT (Control Objectives for Information and related Technology)

Q 12) What are the four levels of documentation that results from the implementation of ISMS.

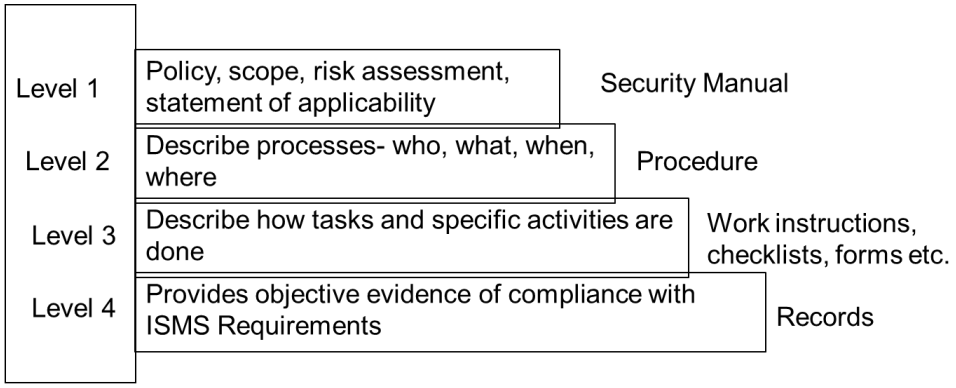
An Information security management systems (ISMS) is a mechanism that works with security related practices through policies, standards and procedures.

The objective of ISMS is to provide a systematic approach to managing sensitive information in order to protect it.

It encompasses employees, processes and information

An ISMS is depicted in figure.

Security threats must be managed and controlled establishing a global policy that is broad security policy with management involvement helps to do this. While doing this, four levels of documentation emerge as shown in figure



Documentation levels in information security management system

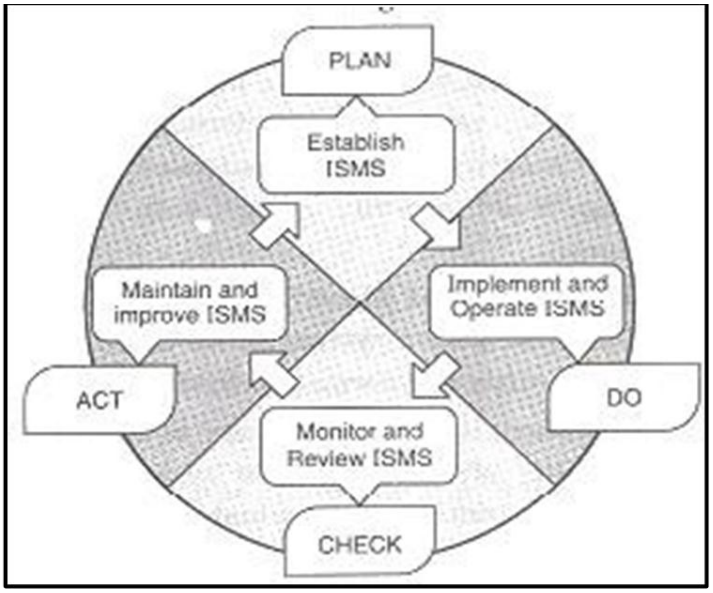
Q .13) Explain ISO 27001 with PDCA Approach

ISO 27001

ISO 27001 is an ISM standard. Its purpose is to help organizations to stablish and maintain an ISMS. It defines a set of requirements that must be met. It describes a 6 stage process:

1) Define an InfoSec policy
2) Define the scope of the ISMS
3) Preform a security assessment
4) Manage the identified risk
5) Select controls to be implemented and applied
6) Prepare a statement of applicability (SoA)

The Plan-Do-Check-Act (PDCA) approach described by ISO 27001 is shown in fig



PDCA Model

1. PLAN-Establish Context:
   i) Define ISMS scope
   ii) Define policy
   iii) Identify Risks
   iv) Assess risks
   v) Select control objectives
2. DO- Implement and Operate
   i) Implement risk treatment plan
   ii) Deploy controls
3. CHECK - Monitor and Review
   i) Monitor processes
   ii) Regular reviews
   iii) Internal audits
4. ACT- Maintain and improve
   i) Implement improvements
   ii) Corrective actions
   iii) Preventive actions
   iv) Communicate with stakeholders

As can be seen, ISO 27001 is an ISMS development methodology and it explains how to create ISMS.

Q 14) Explain ISO 20000 with its two specifications

- ISO 20000

ISO 20000 was originally developed to reflect best practice guidance contained within the ITIL framework.

It is comprised of two parts: a specification for ITSM (Information Technology Service Management) and a code of practice for service management.

ISO/ International Electromechanical Commisssion (IEC) 20000 is the first international standard for ITSM . It consists of two sections:

ISO 20000-1 (Part 1) promotes the adoption of an integrated process approach to effectively deliver managed services to meet the business and customer requirement. It comprises 10 sections:

1. Scope
2. Terms and Definitions
3. Planning and implementing service management
4. Requirements for a Management system
5. Planning and Implementing new or changed services
6. Service Delivery process
7. Relationship Processes
8. Control Processes
9. Resolution processes
10. Release Process

ISO 20000-2 (Part 2) is a code of practice and describes the best practices for service management within the scope of ISO 20000-1. It comprises the same sections as Part -1 but excludes the 'Requirements for a management System'.

Q 15) Write a note on BS 25999

- BS 25999 (British Standard)

  BS 25999 is a two-part British Standard that illustrates what organizations should do to establish demonstrably robust business continuity processes, and how they can evaluate their own processes or those of others who they depend on.

  Part 1: Code of Practice (BS 25999-1:2006) was published in November 2006. It is in the form of guidance and recommendations that illustrate how to develop and maintain a robust BCM system based on good practice.

  - BS25999-1 establishes the process, principles and terminology of BCM.
  - It provides a basis for understanding, developing and implementing business continuity within an organisation and in that organisation's dealings with suppliers, customers and other organisations.
  - It enables the organisation to measure its own and others BCM capabilities in a consistent and recognised manner.
  - It applies to organisations of all sizes and sectors and is intended to be used by anyone who has responsibilities for business operations or the provision of services.

  Part 2: Specification (BS 25999-2:2007) was published in November 2007. It defines requirements for a management systems approach to BCM, against which organizations can be measured formally or informally.

  - BS 25999-2 specifies requirements for "planning, establishing, implementing, operating, monitoring, reviewing and improving a documented Business Continuity

- Management System (BCMS) within the context of managing an organisation's overall business risks". It contains requirements that can be audited against, thus establishing an ability to evaluate the robustness of the BCMS in a consistent manner.

Q 16) Explain the use of PCI DSS

- **PCI DSS (Payment Card Industry Data Security Standard)**

The PCI Security Standards Council offers PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents. The purpose of the Standard is to decrease payment card fraud across the internet and increase credit card data security.

The PCI DSS applies across the whole of organization or to a subset of the organization that transmits or stores the cardholder data away from the rest of the organization.

Tools to assist organizations validate their PCI DSS compliance include Self Assessment Questionnaires.

For device vendors and manufacturers, the Council provides the PIN Transaction Security (PTS) requirements, which contains a single set of requirements for all personal identification number (PIN) terminals, including POS devices, encrypting PIN pads and unattended payment terminals.

To help software vendors and others develop secure payment applications, the Council maintains the Payment Application Data Security Standard (PA-DSS) and a list of Validated Payment Applications.

• PCI DSS Structure is made up of six key sections:
  – Build and Maintain a Secure Network
  – Protect Cardholder Data
  – Maintain a Vulnerability Management Program
  – Implement Strong Control Measures
  – Regularly Monitor and Test Networks
  – Maintain an Information Security Policy

Q 17) Explain the ITIL framework in detail

ITIL (Information Technology Infrastructure Library)

- ITIL is the most widely adopted approach for IT Service Management in the world. It provides a practical, no-nonsense framework for identifying, planning, delivering and supporting IT services to the business.
- Since ITIL is an approach to IT 'service' management, the concept of a service must be discussed. A service is something that provides value to customers. Services that customers can directly utilize or consume are known as business services. An example of a business service that has common applicability across many industries would be Payroll. Payroll is an IT service that is used to consolidate information, calculate compensation and generate pay cheques on a regular basis, and which relies on other business services such as 'time tracking' or 'benefits administration' to provide the extra information necessary for its calculations.
- In order for Payroll to run, it is supported by a number of technology or 'infrastructure' services. An infrastructure service does its work in the background, so that the business does not directly interact with it, but nevertheless this service is necessary as

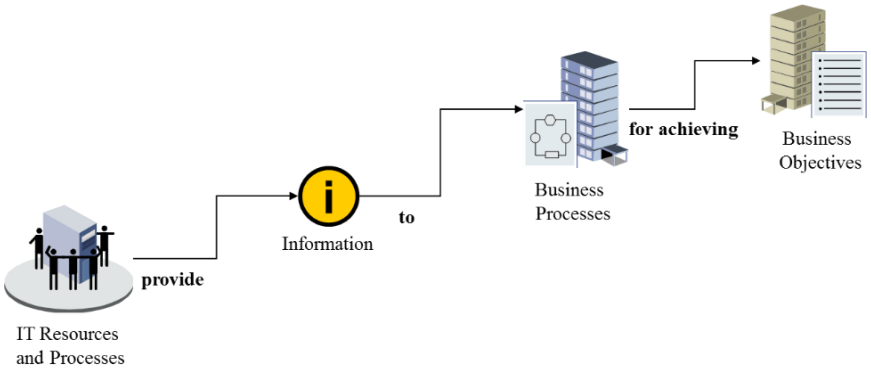
part of the overall value chain to the business service. 'Server administration', 'database administration' and 'storage administration' are all examples of infrastructure services required for the successful delivery of the Payroll business service.

- IT organizations have traditionally focused on managing the infrastructure services and technology silos.
- ITIL suggests a more holistic approach to managing services from end to end. Managing the entire business service along with its underlying components in a cohesive manner ensures that every aspect of a service is considered (and not just the individual technology silos) so that the required functionality (or utility) and service levels (or warranty) are delivered to the business customer. With respect to Payroll, this means accurate pay cheques for all employees, and service levels delivered within a certain timeframe, properly secured, and available when necessary.

Q.18) Describe COBIT framework.

COBIT (The Control Objectives for Information and Related Technology)

- It is a control framework that links IT initiatives to business requirements, organizes IT activities into a generally accepted process model, identifies the major IT resources to be leveraged and defines the management control objectives to be considered.
- COBIT is a framework developed by ISACA (Information System Audit and Control Association) in the year 1996 for IT management and IT governance.
- COBIT is a set of guidance materials for IT governance that allows managers to bridge the gap between control requirements, technical issues and business risks.
- The main aim of COBIT 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, IT professionals and assurance.



COBIT Framework Principles

-
- The COBIT framework is based on the following principle: To provide the information that the organization requires to achieve its objectives, the organization requires investing in and managing and controlling IT Resources using a structured set of processes to provide the services which deliver the required enterprise information.

- Managing and controlling information are at the heart of the COBIT framework and help to ensure alignment to business requirement.
- COBIT defines IT activities in a generic process model within four domains. These domains are:
  1. Plan and Organize
  2. Acquire and Implement
  3. Deliver and Support
  4. Monitor and Evaluate
- COBIT supports IT governance by providing a framework to ensure that
  1. IT is aligned with the business (Strategic Alignment)
  2. IT enables the business and maximizes benefits (Value Delivery)
  3. IT resources are used responsibly.(Resource Management)
  4. IT risks are managed appropriately (Risk Management)

COBIT and IT Governance