

**Internal Assessment Test I – March. 2018- Scheme of evaluation and solution**

|       |                                  |            |           |            |     |
|-------|----------------------------------|------------|-----------|------------|-----|
| Sub:  | INFORMATION AND NETWORK SECURITY | Sub Code:  | 10CS835   | Branch:    | CSE |
| Date: | 13 / 03 / 2018                   | Duration:  | 90 mins   | Max Marks: | 50  |
|       |                                  | Sem / Sec: | 8 (A,B,C) |            | OBE |

**Answer Any FIVE FULL Questions**

**1 (a)** What are the components of contingency planning? Describe briefly the important steps involved in the recovery process after the extent of damage caused by an incident has been assessed?

|       |     |       |
|-------|-----|-------|
| MARKS | CO  | RBT   |
| [10]  | CO1 | L1,L2 |

**Components of Contingency Planning**



37

An incident is any clearly identified attack on the organization’s information assets that would threaten the assets’ confidentiality, integrity, or availability. An incident response (IR) plan addresses the identification, classification, response, and recovery from an incident. A disaster recovery (DR) plan addresses the preparation for and recovery from a disaster, whether natural or man-made. A business continuity (BC) plan ensures that critical business functions continue if a catastrophic incident or disaster occurs. The primary functions of these three types of planning are as follows:

The IR plan focuses on immediate response, but if the attack escalates or is disastrous (e.g., fire, flood, earthquake, or total blackout) the process moves on to disaster recovery and the BC plan.

The DR plan typically focuses on restoring systems at the original site after disasters occur, and as such is closely associated with the BC plan.

The BC plan occurs concurrently with the DR plan when the damage is major or ongoing, requiring more than simple restoration of information and information resources. The BC plan establishes critical business functions at an alternate site.

**RECOVERY**

Full recovery from an incident requires that you perform the following:

1. Identify the vulnerabilities that allowed the incident to occur and spread. Resolve them.
2. Address the safeguards that failed to stop or limit the incident, or were missing from the system in the first place. Install, replace, or upgrade them.
3. Evaluate monitoring capabilities (if present). Improve their detection and reporting

methods, or simply install new monitoring capabilities.

4. Restore the data from backups. See the Technical Details boxes on the following topics for more information:

- (1) data storage and management,
- (2) system backups and recovery,
- (3) redundant array of independent disks (RAID).

Restoration requires the IR team

to understand the backup strategy used by the organization, restore the data contained in

backups, and then recreate the data that were created or modified since the last backup.

5. Restore the services and processes in use. Compromised services and processes must be examined, cleaned, and then restored. If services or processes were interrupted during

the process of regaining control of the systems, they need to be brought back online.

6. Continuously monitor the system. If an incident happened once, it can easily happen

again. Just because the incident is over doesn't mean the organization is in the clear.

Hackers frequently boast of their abilities in chat rooms and dare their peers to match

their efforts. If word gets out, others may be tempted to try their hands at the same or

different attacks. It is therefore important to maintain vigilance during the entire IR

process.

7. Restore the confidence of the organization's communities of interest. It may be advisable to issue a short memorandum that outlines the incident and assures everyone that it was handled and the damage controlled. If the incident was minor, say so. If the incident was major or severely damaged the systems or

data, reassure the users that they can expect operations to return to normal shortly. The objective is not to placate or lie, but to prevent panic or confusion from causing additional disruptions to the operations of

the organization.

**2 (a) What are the three components of the CIA triangle? What are they used for?**

[4]

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. Confidentiality is roughly equivalent to [privacy](#). Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people.

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality).

Availability is best ensured by rigorously maintaining all [hardware](#), performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It's

|     |    |
|-----|----|
|     |    |
| CO1 | L1 |



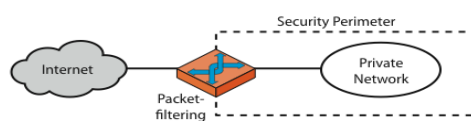
| Components of An ISSP |   |
|-----------------------|---|
| 1.                    | Statement of policy<br>a. Scope and applicability<br>b. Definition of technology addressed<br>c. Responsibilities   |
| 2.                    | Authorized access and usage of equipment<br>a. User access<br>b. Fair and responsible use<br>c. Protection of privacy   |
| 3.                    | Prohibited usage of equipment<br>a. Disruptive use or misuse<br>b. Criminal use<br>c. Offensive or harassing materials<br>d. Copyrighted, licensed, or other intellectual property<br>e. Other restrictions |
| 4.                    | Systems management<br>a. Management of stored materials<br>b. Employer monitoring<br>c. Virus protection<br>d. Physical security<br>e. Encryption   |
| 5.                    | Violations of policy<br>a. Procedures for reporting violations<br>b. Penalties for violations   |
| 6.                    | Policy review and modification<br>a. Scheduled review of policy procedures for modification<br>b. Legal disclaimers   |
| 7.                    | Limitations of liability<br>a. Statements of liability<br>b. Other disclaimers as needed  |

3 (a) Explain the categories of firewall based on the processing modes and depict it using OSI layer?

[8]

CO2 L1,L2

### PACKET FILTERING

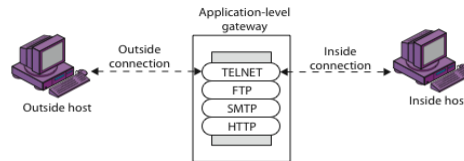


(a) Packet-filtering router

- Applies a set of rules to each incoming IP packet and then forwards or discards the packet
  - Filter packets going in both directions
  - The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
  - Two default policies (discard or forward)
  - Address Restrictions
- ⊙ Static packet filtering firewall  
Static filtering requires that the filtering rules be developed and installed within the firewall.
  - ⊙ Dynamic packet filtering  
Dynamic packet filtering filters packets based on:

- ⊙ Administrator defined rules governing allowed ports and IP addresses at the network and transport layers of the OSI network model.
- ⊙ Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- ⊙ Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of Authentication
- ⊙ Possible attacks and appropriate countermeasures
  - IP address spoofing
  - Source routing attacks

### APPLICATION LEVEL



(b) Application-level gateway

Has full access to protocol user requests service from proxy ,proxy validates request as legal then actions request and returns result to user .

Need separate proxies for each service

E.g., SMTP (E-Mail)

NNTP (Net news)

DNS (Domain Name System)

NTP (Network Time Protocol)

custom services generally not supported

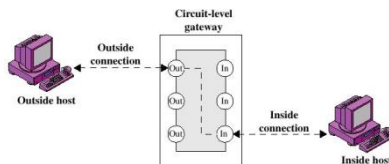
Advantages:

- Higher security than packet filters
- Only need to scrutinize a few allowable applications

Disadvantages:

- Additional processing overhead on each connection (gateway as splice point)

### CIRCUIT GATEWAY



- ⊙ Circuit-level Gateway
  - It does not control the traffic flow between one network and the other rather
  - It prevents direct connection between one network and the other .
- ⊙ Tunnels
- ⊙ Allows only authorized traffic
  - ⊙ An example is the SOCKS package

### MAC LAYER FIREWALL

operates on OSI Layer 2 and bases its filtering decision on devices'

**MAC/NIC addresses**

MAC addresses of specific hosts are included in ACL, allowing only specific packets to be sent to/from these hosts and blocking others not as widely used as other types of firewalls **only used within a single-authority LAN - MAC addresses get stripped off on each 'hop'**.

**HYBRID**

Hybrid Firewall – combines elements of other types of firewalls

- ⊙ Typically implies the use of two or more separate firewall devices.
- ⊙ Allows an organization to make security improvements without completely replacing its existing firewalls

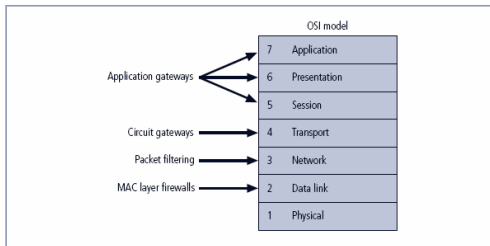


FIGURE 6-5 Firewall Types and the OSI Model

(b) **What are virtual private networks and its characteristics? Name the two modes of VPN** [2]

CO2 L1,L2

A VPN or Virtual Private Network is a network connection that enables you to create a secure connection over the public Internet to private networks at a remote location.

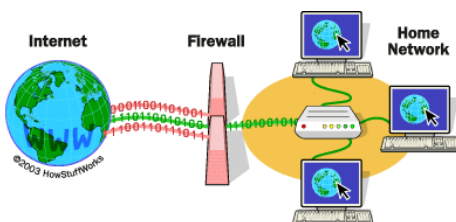
Encapsulation  
Encryption  
Authentication

2 modes:  
Transport mode  
Tunnel mode

4 (a) **What is a firewall? Show the working of a screened host and dual homed firewall?** [10]

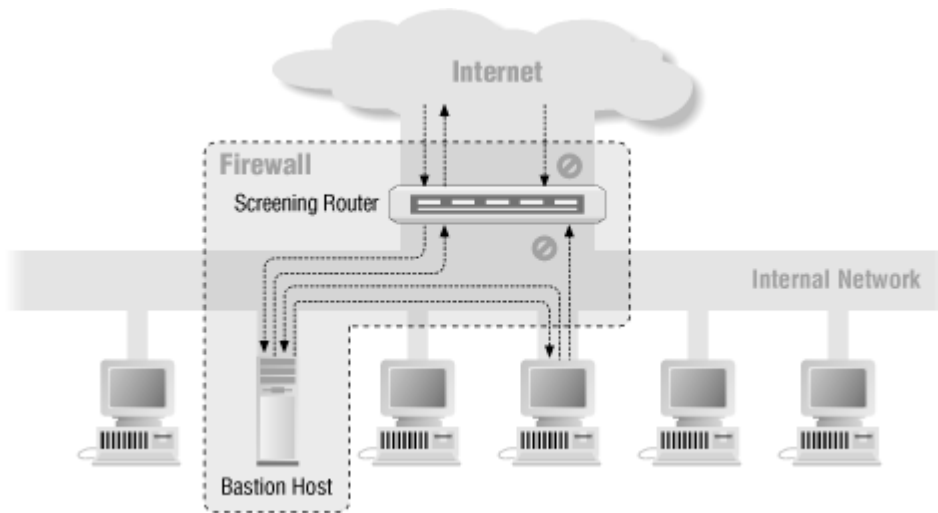
CO2 L1,L3

A **firewall** is a [network security](#) system that [monitors](#) and controls the incoming and outgoing [network traffic](#) based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the [Internet](#), that is assumed not to be secure or trusted.



SCREENED HOST

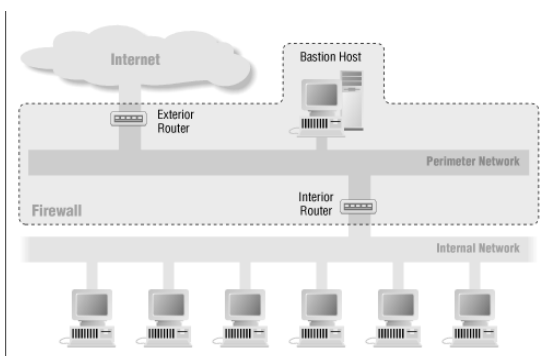
Screened host firewalls combine the packet-filtering router with a separate, dedicated firewall, such as an application proxy server. This approach allows the router to prescreen packets to minimize the network traffic and load on the internal proxy. The application proxy examines an application layer protocol, such as HTTP, and performs the proxy services. This separate host is often referred to as a **bastion host**; it can be a rich target for external attacks and should be very thoroughly secured. Even though the bastion host/application proxy actually contains only cached copies of the internal Web documents, it can still present a promising target, because compromise of the bastion host can disclose the configuration of internal networks and possibly provide attackers with internal information. Since the bastion host stands as a sole defender on the network perimeter, it is commonly referred to as the **sacrificial host**.



#### DUAL HOMED HOST

When this architectural approach is used, the bastion host contains two NICs (network interface cards) rather than one, as in the bastion host configuration.

One NIC is connected to the external network, and one is connected to the internal network, providing an additional layer of protection. With two NICs, all traffic *must* physically go through the firewall to move between the internal and external networks. Implementation of this architecture often makes use of NAT. As described earlier in this chapter, NAT is a method of mapping real, valid, external IP addresses to special ranges of no routable internal IP addresses.

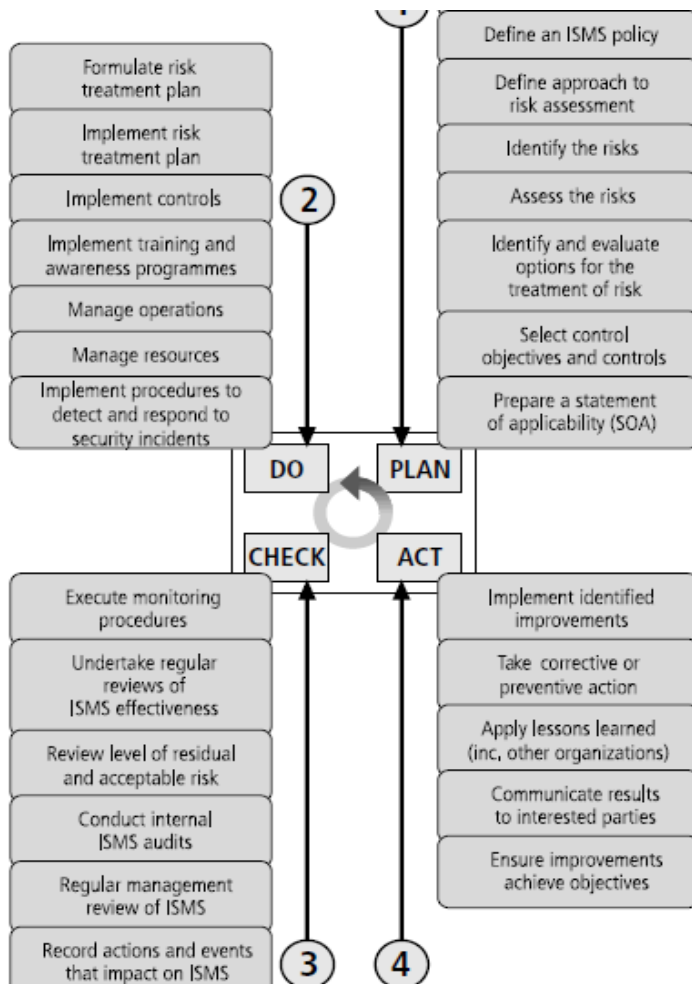
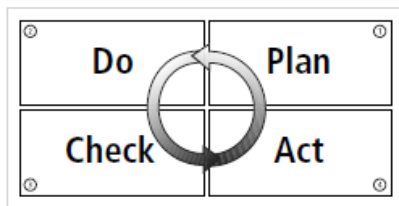


5 (a) Explain in detail the Information security Blue print?

[10]

CO1 L2

This **security blueprint** is the basis for the design, selection, and implementation of all security program elements including policy implementation, ongoing policy management, risk management programs, education and training programs, technological controls, and maintenance of the security program. The security blueprint, built on top of the organization's information security policies, is a scalable, upgradeable, comprehensive plan to meet the organization's current and future information security needs. It is a detailed version of the **security framework**, which is an outline of the overall information security strategy for the organization and a roadmap for planned changes to the information security environment of the organization. The blueprint specifies the tasks and the order in which they are to be accomplished.

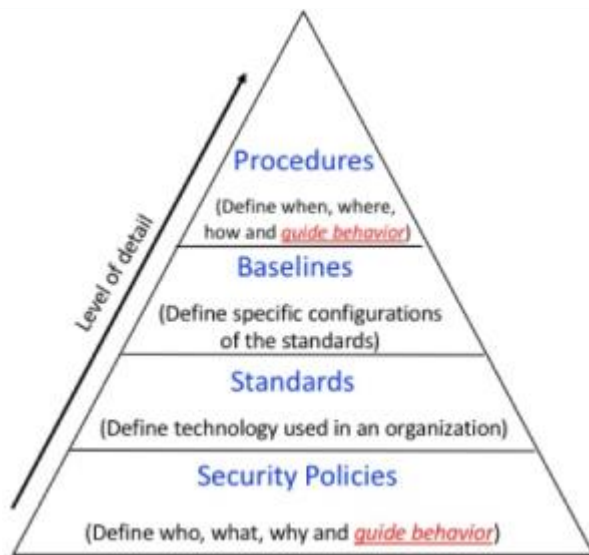


6 (a) With a block schematic diagram explain how policies, standards, practices, procedures and guidelines are related?

[7]

CO1 L2





Policies are put in place to support the mission, vision, and strategic planning of an organization.

The **mission** of an organization is a written statement of an organization's purpose. The

**vision** of an organization is a written statement about the organization's goals—where will The organization be in five years? In ten? Strategic planning is the process of moving the organization toward its vision. The meaning of the term **security policy** depends on the context in which it is used. Governmental agencies view security policy in terms of national security and national policies to deal with foreign states. A security policy can also communicate a credit card agency's method for processing credit card numbers. In general, a security policy is a set of rules that protect an organization's assets. An **information security policy** provides rules for the protection of the information assets of the organization.

1. Enterprise information security policies
2. Issue-specific security policies
3. Systems-specific security policies

For a policy to be effective and thus legally enforceable, it must meet the following criteria:

**Dissemination (distribution)**—The organization must be able to demonstrate that the

policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution

**Review (reading)**—The organization must be able to demonstrate that it disseminated

the document in an intelligible form, including versions for illiterate, non-English reading,

and reading-impaired employees. Common techniques include recording the policy

in English and other languages.

**Comprehension (understanding)**—The organization must be able to demonstrate the employee understood the requirements and content of the policy. Common techniques

include quizzes and other assessments.

**Compliance (agreement)**—The organization must be able to demonstrate that the employee agrees to comply with the policy, through act or affirmation. Common techniques include logon banners which require a specific action (mouse click or keystroke) to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.

**Uniform enforcement**—The organization must be able to demonstrate that the

policy has been uniformly enforced, regardless of employee status or assignment.

(b) What are the types of security policies? Where would each be used?

[3]

EISP  
IISP  
SSSP

CO1 L1

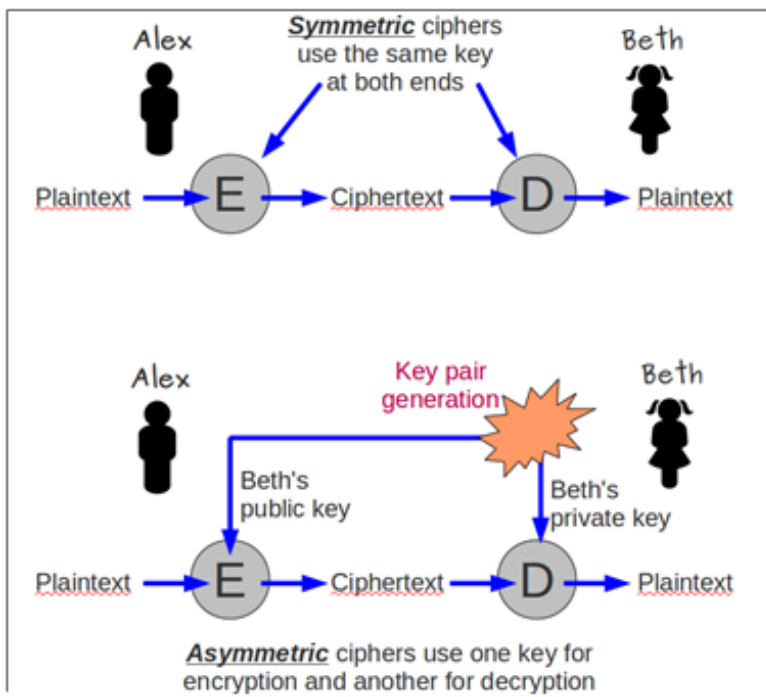
7 (a)

What is an encryption? Discuss the symmetric and asymmetric encryption methods. explain caesar cipher technique ,Also show the Encryption/Decryption for the text “MEET ME AFTER THE PARTY”?

[5+5]

CO3 L1,L2,L3

Encryption is the conversion of electronic data into another form, ciphertext, which cannot be easily understood by anyone except authorized parties.



**Symmetric-key algorithms** are algorithms for **cryptology** that use the **cryptographic** keys for both **encryption** of plaintext and decrypt ciphertext. The keys may be identical or there may be a simple transformation between the two keys.

Public key **cryptology**, or **asymmetric cryptology**, is any **cryptology** system that uses pairs of keys: public keys which may be disseminated and private keys which are known only to the owner.

The earliest known, and the simplest, use of a substitution cipher was by J Caesar. The Caesar cipher involves replacing each letter of the alphabet with a letter standing three places further down the alphabet. For example,

plain: meet me after the toga party  
cipher: PHHW PH DIWHU WKH WRJD SDUWB

Note that the alphabet is wrapped around, so that the letter following Z is A.  
We can define the transformation by listing all possibilities, as follows:

plain: a b c d e f g h i j k l m n o p q r s t u v w x y z  
cipher: d e f g h i j k l m n o p q r s T u v w x y z a b c

A shift may be of any amount, so that the general Caesar algorithm is

$$C = E(k, p) = (p + k) \bmod 26$$

where  $k$  takes on a value in the range 1 to 25. The decryption algorithm is simply

$$p = D(k, C) = (C - k) \bmod 26$$

If it is known that a given cipher text is a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys. Three important characteristics of this problem enabled us to use a brute force cryptanalysis:

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.

Problem solution: PHHW PH DIWHU WKH SDUWB