USN | | | | | | | | | | |

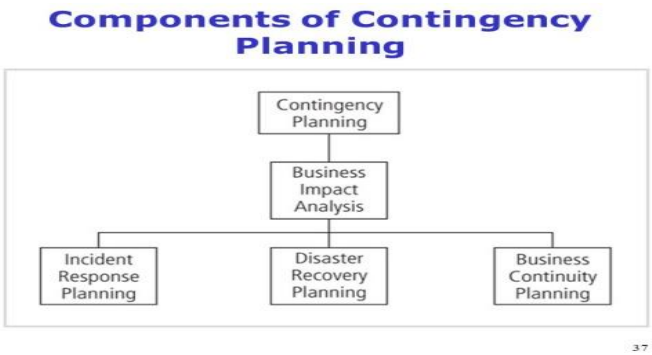
Internal Assesment Test I – March. 2018- **Scheme of evaluation and solution**

Sub:	INFORMATION AND NETWORK SECURITY					Sub Code:	10IS835	Branch:	ISE
Date:	13 / 03 / 2018	Duration:	90 mins	Max Marks:	50	Sem / Sec:	8 (A,B)		OBE

Answer Any FIVE FULL Questions MARKS CO RBT

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? [10] CO1 L1,L2

(Drawing the components carries 3 marks)
(Explanation on 3 types carries 3 marks)
(Explanation on recovery carries 4 marks)



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]	CO1	L1

(Explanation with Diagram carries 2 marks each)

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 also important to keep current with all necessary system upgrades.

(b) Explain Issue Specific Security Policy? [6] CO1 L2

(Explanation carries 3 Marks)

(Mention the Components carries 3 Marks)

– As various technologies and processes are implemented, certain guidelines are needed to use them properly
– The ISSP:
– addresses specific areas of technology like
– Electronic mail
– Use of the Internet
– Specific minimum configurations of computers to defend against worms and viruses.
– Prohibitions against hacking or testing organization security controls.
– Home use of company-owned computer equipment.
– Use of personal equipment on company networks
– Use of telecommunications technologies (FAX and Phone)
– Use of photocopy equipment.
_ requires frequent updates
_ contains an issue statement on the organization's position on an issue
– There are a number of approaches to take when creating and managing ISSPs within an
organization.
– **Three approaches**

_ Independent ISSP documents, each tailored to a specific issue.
_ A single comprehensive ISSP document covering all issues.
_ A modular ISSP document that unifies policy creation and administration, while maintaining each specific issue's requirements.
– The independent document approach to take when creating and managing ISSPs typically has a scattershot effect.
– Each department responsible for a particular application of technology creates a policy
governing its use, management, and control.
– This approach to creating ISSPs may fail to cover all of the necessary issues, and can lead
to poor policy distribution, management, and enforcement.
– The single comprehensive policy approach is centrally managed and controlled.
– With formal procedures for the management of ISSPs in place, the comprehensive policy
approach establishes guidelines for overall coverage of necessary issues and clearly
identifies processes for the dissemination, enforcement, and review of these guidelines.
– Usually, these policies are developed by those responsible for managing the information

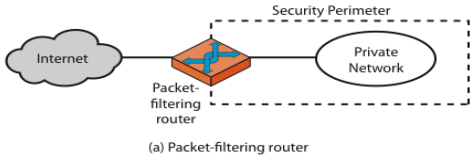
technology resources.
– The optimal balance between the independent and comprehensive ISSP approaches is the modular approach.

COMPONENTS OS ISSP

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

(Any 4 Type of firewall explanation with diagram carries 2 marks)
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:

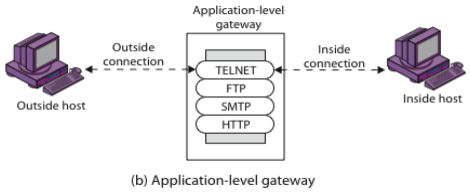
⦿ Administrator defined rules governing allowed ports and IP addresses at the network and transport layers of the OSI network model.

⦿ 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



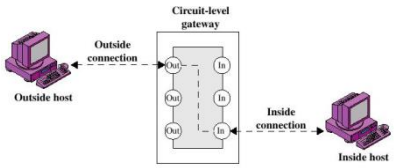
(b) Application-level gateway

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

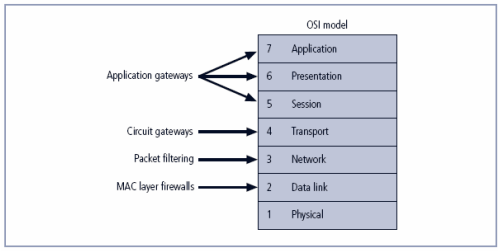


FIGURE 6-5 Firewall Types and the OSI Model

(b) What are virtual private networks and its characteristics? Name the two modes of VPN [2] CO2 L1,L2

(Definition of firewall carries 1 mark)

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.

(Character tics of firewall carries 1 mark)

Encapsulation
Encryption
Authentication

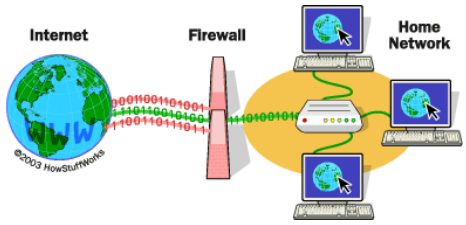
(Mention 2 Modes of VPN Carries 1 marks)

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

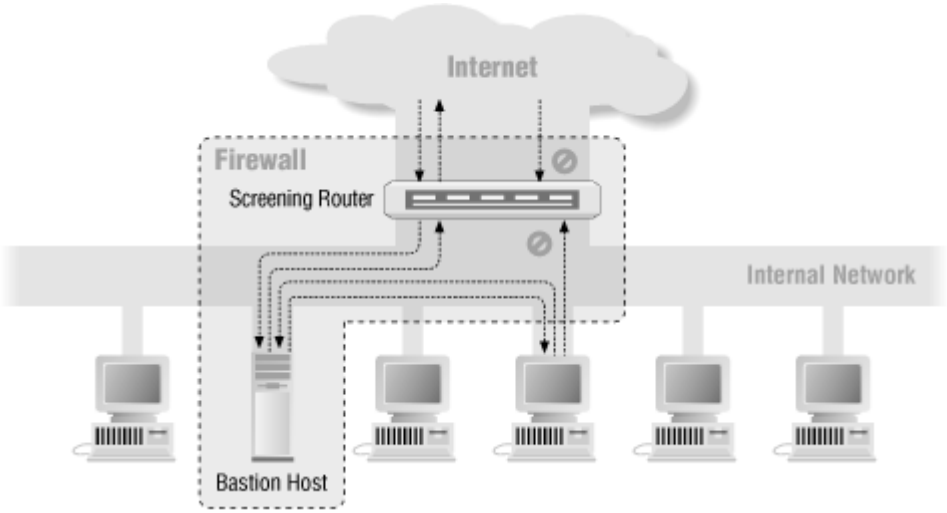
(Each Firewall with working and diagram carries 5 marks)

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.



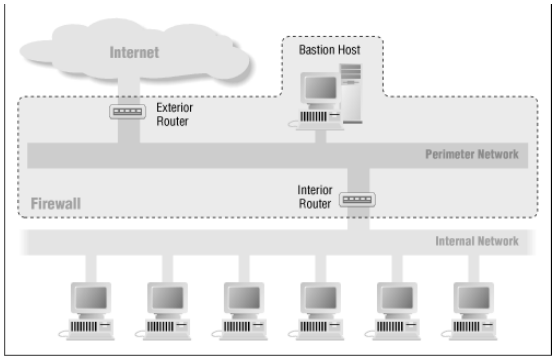
SCREENED HOST

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.

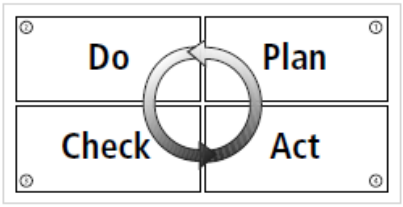


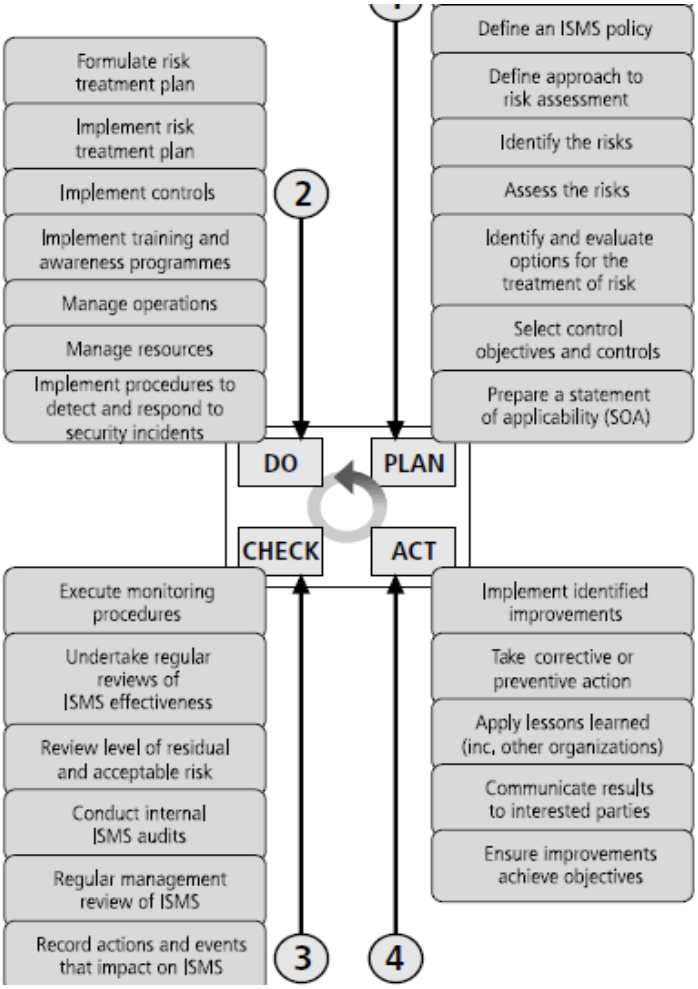
5 (a) Explain in detail the Information security Blue print? [10] CO1 L2

(Explanation with Diagram carries 6 +4 marks each)

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,

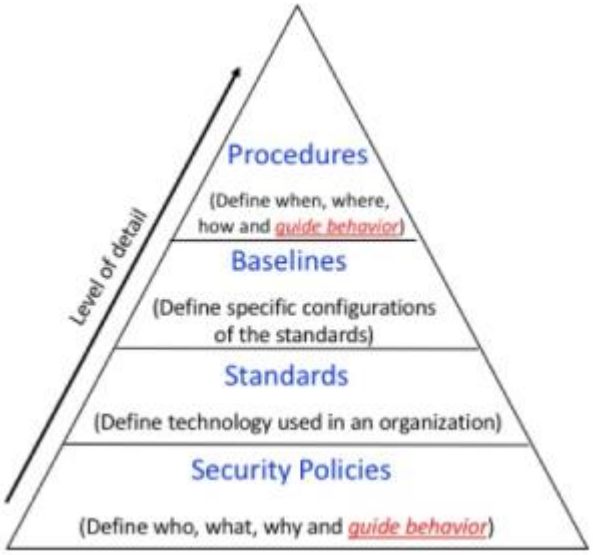
which is an outline of the overall information security strategy for the organization and a roadmap for planned changes to the information security environment of the organization.The blueprint specifies the tasks and the order in which they are to be accomplished.





6 (a) With a block schematic diagram explain how policies, standards, practices, procedures and guidelines are related? [7] CO1 L2

(Explanation with Diagram carries 4 +3marks each)



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? (**Each policy carries 1 mark each)**	[3]	CO1	L1	