2 marks Questions and Answers

UNIT -I

1. What is Information security?

Information security includes the broad areas of information security management, computer and data security, and network security.

2. What is C.I.A triangle in detail (or what are components of Information security)

The C.I.A. triangle - confidentiality, integrity, and availability - has expanded into a more comprehensive list of critical characteristics of information. Components are management of information security, computer & data security, network security, policy

3. What are the characteristics of information?

Confidentiality - Integrity -Availability - Privacy - Identification - Authentication - Authorization - Accountability -Accuracy - Utility – Possession

4. What is a threat?

A threat is an object, person, or other entity that represents a constant danger to an asset.

5. **What is spoofing**?

Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

6. **Explain Trojan horses and their attack**?.

They are software programs that hide their true nature, and reveal their designed behavior only when activated

7. What is back door or trap door?

This allows the attacker to access the system at will with special privileges. Examples: Subseven and Back Orifice.

8. **What is an attack?**

An attack is the deliberate act that exploits vulnerability.• It is accomplished by a threat agent that damages or steals an organization's information• or physical asset. An exploit is a technique to compromise a system.¬ Vulnerability is an identified weakness of a controlled system with controls¬ that are not present or are no longer effective.

9. What is Brute force attack?

The application of computing and network resources to try every possible combination of• options of a password is called a brute force attack. This is often an attempt to repeatedly guess passwords to commonly used accounts, it is• sometimes called a password attack.

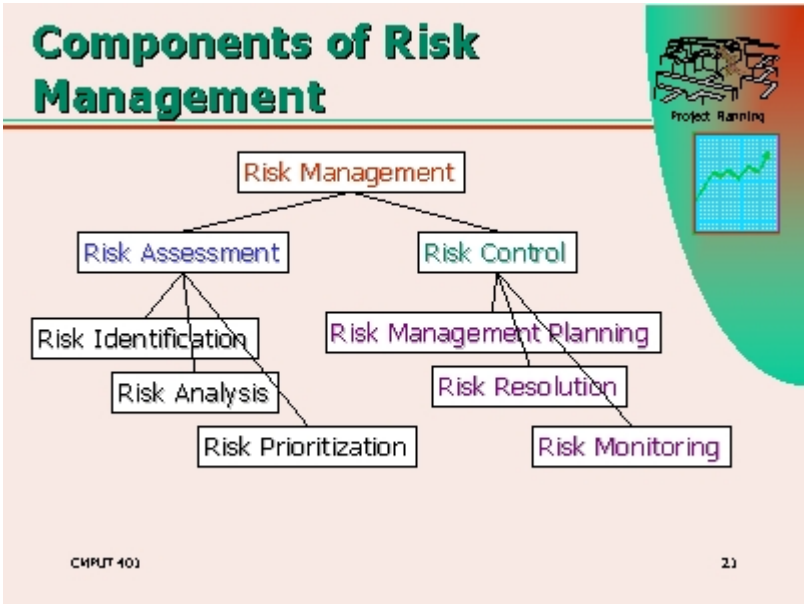
10. **Explain DoS and DDoS In a denial-of-service (DoS) attack**

The attacker sends a large number of connection or information requests to a target¬ So many requests are made that the target system cannot handle them successfully¬ along with other, legitimate requests for service. This may result in a system crash, or merely an inability to perform ordinary¬ functions. A distributed denial-of-service (DDoS) is An attack in which a coordinated stream of requests is launched against a target from¬ many locations at the same time. Most DDoS attacks are preceded by a preparation phase in which many systems,¬ perhaps thousands, are compromised. The compromised machines are turned into zombies, directed towards the target,¬ and executed remotely (usually by a transmitted command) by the attacker.

UNIT 2

1. What is risk management? What are the components of risk management.

• Risk management is Evaluating Risk Control, Determining Feasible Solutions, Acquiring or Installing Needed Controls, Ensuring the controls remain Effective



2. What are the factors of risk?

Risk is likelihood of occurrence of vulnerability multiplied by value of information asset minus percentage of risk mitigated by current controls plus uncertainty of current knowledge of vulnerability

3. What are the types of access controls ?(or)

4. What is risk control cycle

1. Avoidance • Application of policy • Training • Application of tech
2. Transference
3. Mitigation • Incident Response plan • Disaster Recovery plan • Business Continuity plan
4. Acceptance Risk Appetite Cost Benefit Analysis: Using appropriate feasibility

5. What is CBA?

Benefit is determined by valuing the info asset¬ & then determining how much of value is at risk Or how much risk is there for asset C.B.A=ALE(PRIOR)-ALE(POST)-ACS • SLE SLE=asset value * exposure factor • ALE ALE=SLE * ARO

6. What is base lining and benchmarking?

• Instead of analyzing current situation following the strategies of other organizations is Bench marking Metrics Based Measures¬ Process Based Measures¬ • What is done more stressed than how it is done

UNIT- 3

1. Define policy, standard and practice with a diagram

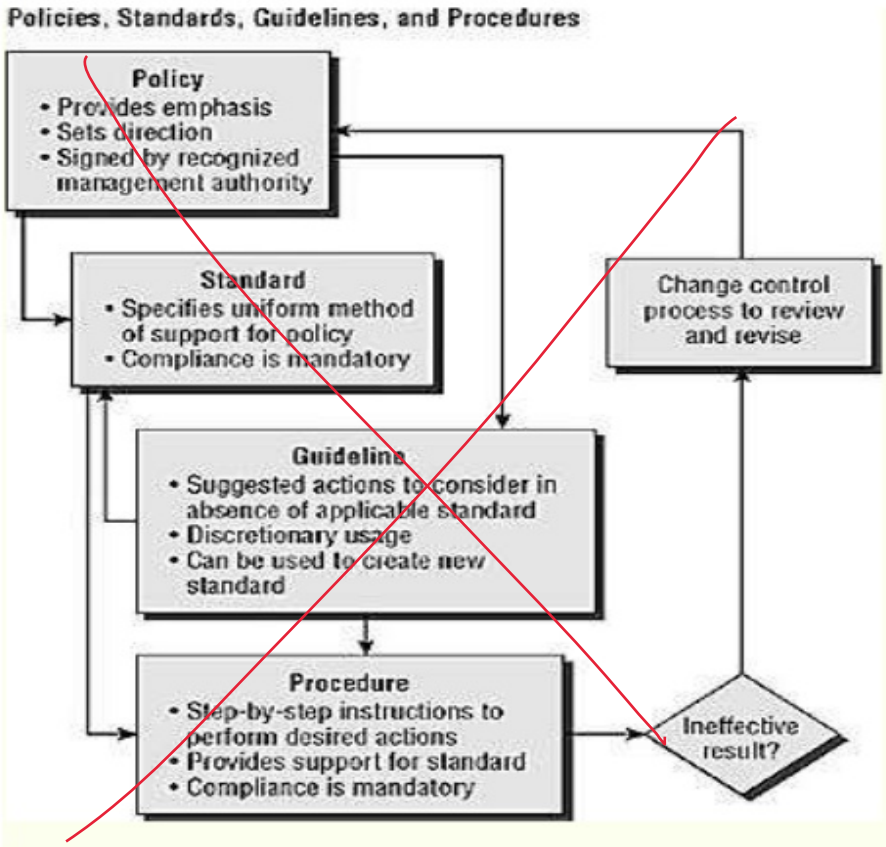


Figure 1: The relationship between a policy, standard, guideline, and procedure

2. What are the three information security policies?

Enterprise Information Security Policy (EISP), Issue-Specific Security Policy, SystemsSpecific Policy (SysSP).

3. What is security blueprint?

Security Blueprint is the basis for design, selection, and implementation of a. all security policies, b. education and training programs, and c. technological controls

4. Explain spheres of security in Hybrid framework?

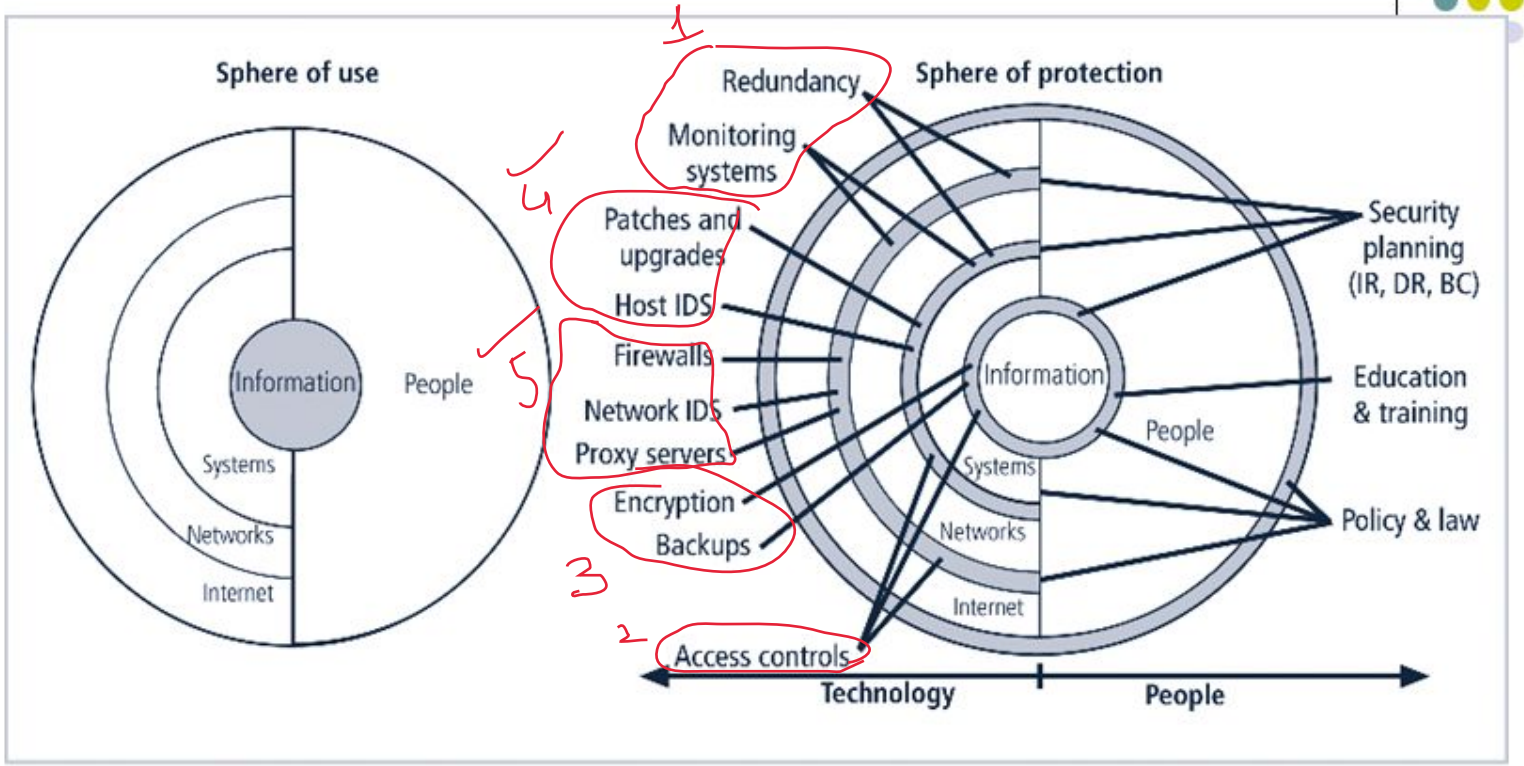
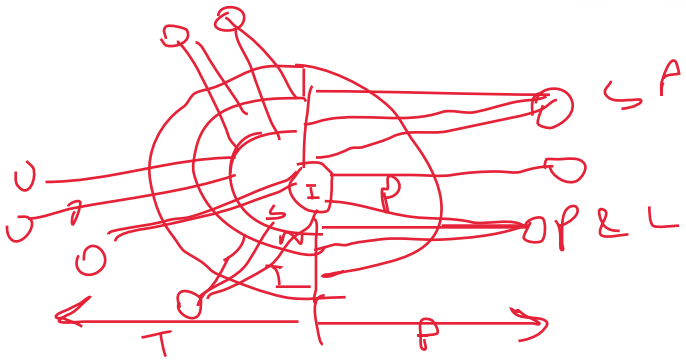


FIGURE 5-15 Spheres of Security



5. What is DMZ?

a. Buffer against outside attacks

b. No mans land between computer and world

c. Web servers often go here

6. What is a proxy server?

a. Performs actions of behalf of another system

b. Configured to look like a web server

c. Assigned the domain name

d. Retrieves and transmits data

e. Cache server

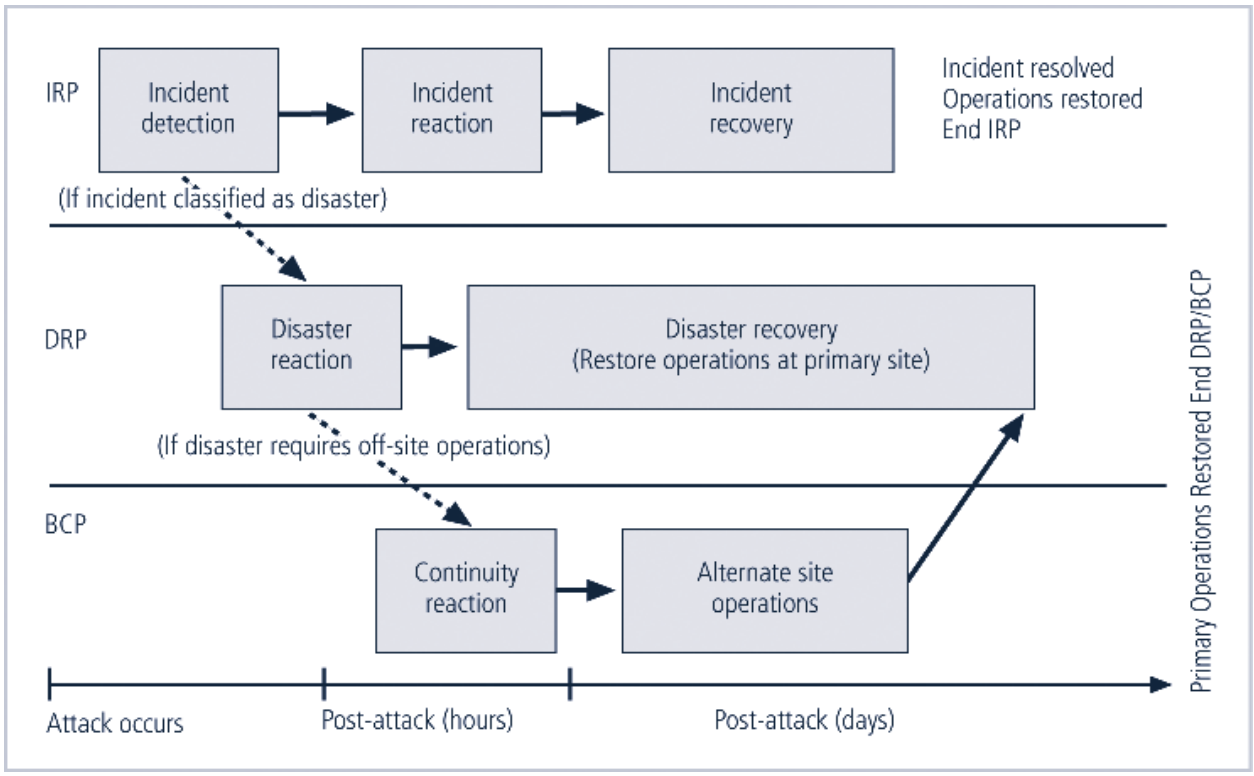
7. **What is a firewall? What are its categorizations?**

A firewall prevents specific types of information from moving between the outside world, known as the un-trusted network, and the inside world, known as the trusted network. Firewalls can be categorized by processing mode, development era, or intended structure. The processing modes are: packet filtering, application gateways, circuit gateways, MAC layer firewalls, and hybrids.

8. **What is a vpn? What are its 2 modes?**

A VPN is a private and secure network connection between systems that uses the data communication capability of an unsecured and public network. Its two modes are transport mode and tunnel mode. In transport mode, the data within an IP packet is encrypted, but the header information is not. This allows the user to establish a secure link directly with the remote host, encrypting only the data contents of the packet. In tunnel mode, the organization establishes two perimeter tunnel servers. These servers serve as the encryption points, encrypting all traffic that will traverse an unsecured network.

9. **What is contingency planning? Explain its components?**



10. **What is BIA?**

Investigate & assess impact of various attack

o First risk assessment – then BIA Contingency Planning Incident Response (IRPs) (Focus on immediate response) Disaster Recovery (DRPs) (Focus on restoring system) Business Continuity (BCPs) (Focus establish business functions at alternate site)

o Prioritized list of threats & critical info

o Detailed scenarios of potential impact of each attack o Answers question "if the attack succeeds, what do you do then?"♣

11. What is IRP?

Incident response planning covers identification of, classification of, and response to an incident

12. **What is the process involved in Disaster recovery planning. Explain in few lines.** Provide guidance in the event of a disaster Clear establishment of priorities Clear delegation of roles & responsibilities Alert key personnel Document disaster Mitigate impact Evacuation of physical assets

13. Why do we need Business continuity planning? What do we do in it?

Outlines reestablishment of critical business operations during a disaster that impacts operations If disaster has rendered the business unusable for continued operations, there must be a plan to allow business to continue functioning Development of BCP somewhat simpler than IRP or DRP; consists primarily of selecting a continuity strategy and integrating off-site data storage and recovery functions into this strategy

13. What is crisis management?

Disaster recovery personnel must know their responses without any supporting documentation Actions taken during and after a disaster focusing on people involved and addressing viability of business Crisis management team responsible for managing event from an enterprise perspective and covers: 1. Support personnel and loved ones 2. Determine impact on normal operations 3. Keep public informed

UNIT 4

1. What is IDS?

What are the two IDS and their function. IDSs work like burglar alarms. An IDS operates as either network-based, when the♦ technology is focused on protecting network information assets, or host-based, when the technology is focused on protecting server or host information assets IDSs use one of two detection methods, signature-based or statistical anomaly-based

2. What are packet sniffers and content filters?

A network tool that collects copies of packets from the network and analyzes⎪ them. Can be used to eavesdrop on the network traffic A content filter is a software filter that allows administrators to restrict accessible⎪ content from within a network. The content filtering restricts Web sites with inappropriate content .

3. What is Cryptography?

The science of encryption, known as cryptology, encompasses cryptography and cryptanalysis

4. Explain Symmetric Encryption.

Uses same "secret key" to encipher and decipher message a. Encryption methods can be extremely efficient, requiring minimal processing b. Both sender and receiver must possess encryption key c. If either copy of key is compromised, an intermediate can decrypt and read messages d. Ex: DES, AES, Triple DES

5. Explain Asymmetric Encryption.

Also known as public-key encryption Uses two different but related keys a. Either key can encrypt or decrypt message b. If Key A encrypts message, only Key B can decrypt c. Highest value when one key serves as private key and the other serves as public key Ex: RSA algorithm

6. What are the different encryption operations?

In encryption the most commonly used algorithms include two functions: substitution and transposition In a substitution cipher, you substitute one value for another - monoalphabetic,♦ polyalphabetic The transposition cipher (or permutation cipher) simply rearranges the values within a♦ block to create the ciphertext

7. What is digital signature?

Digital Signatures are encrypted messages that are independently verified by a central facility (registry) as authentic

8. What is a digital certificate?

A digital certificate is an electronic document, similar to a digital signature, attached to a file certifying that this file is from the organization it claims to be from and has not been modified from the original format

UNIT-5

1. What are Information security positions and relationships?

Chief Information Security officer, Security manager- security technician, administrator, security officer.

2. What is CISSP?

The CISSP certification recognizes mastery of an internationally recognized common body of knowledge (CBK) in information security, covering ten domains of information security knowledge: a. Access control systems and methodology b. Applications and systems development c. Business continuity planning d. Cryptography Law, investigation, and ethics

3. What are the different personnel security practices?

a. On-the-Job Security Training b. Security as Part of Performance Evaluation Intentional information compromise can be handled by: c. Separation of duties d. Two-person control e. Job rotation f. Task rotation g. Mandatory vacation h. Principle of least privilege

4. What are employee termination issues?

a. The former employee's access to the organization's systems must be disabled b. The former employee must return all removable media c. The former employee's hard drives must be secured d. File cabinet locks must be changed e. Office door locks must be changed f. The former employee's keycard access must be revoked g. The former employee's personal effects must be removed from the premises h. The former employee should be escorted from the premises, once keys, keycards, and other business property have been turned over

5. What re different employee departure?

Two methods for handling employee out processing, depending on the employee's reasons for leaving, are: a. Hostile departures b. Friendly departures.