****

**CSF 3103**

**Incidence Response and Disaster Recovery**

**Questions Bank**

**FWA Revision**

**Prepared By:**

**Dr. Ebrahim Alhanaee**

**202120**

**Short Answer Questions**

* **Explain the four steps of contingency planning with respect to CP time line.**
* **Evaluate the contingency planning to describe any five purpose of contingency planning policy.**
* **Explain Cold site as an exclusive site resumption strategy - Give any two benefits of using this strategy?**
* **Explain mirroring as a real-time protection and backup strategy.**
* **Explain the differences between Hot-sites and Warm-sites as the site resumption strategies.**
* **Explain “NAS” and “SAN” as supporting technologies for backup and recovery.**
* **Explain any six situations or circumstances to trigger IR plan.**
* **Compose of a list of any three steps for After-Action-Review (AAR) for business contingency planning.**
* **Compose at list of activities to perform as a part of (AAR) for DRP.**
* **Devise a list of any three strategies that can be applied for preparation of DRP with respect to testing and rehearsal.**
* **What is information security?**
* **What is risk management?**
* **What are the component parts of risk management?**
* **What are the basic strategies used to control risk? Define each.**
* **What is a contingency plan?**
* **List and describe the four subordinate functions of a contingency plan.**
* **What is the first step in beginning the contingency planning process?**
* **What are the primary responsibilities of the contingency planning management team (CPMT)?**
* **What is a business impact analysis (BIA), and why is it important?**
* **What are the usual stages in the conduct of the BIA?**
* **What is maximum tolerable downtime (MTD)?**
* **What is recovery time objective (RTO)?**
* **What is recovery point objective (RPO), and how does it differ from recovery time objective?**
* **What are the two major component parts of BRP, and how are they related?**
* **What is the difference between a backup and an archive?**
* **How have cloud computing architectures affected the backup options available for organizations?**
* **What is encompassed in a full backup, a differential backup, and an incremental backup?**
* **What is a redundant array of independent disks (RAID), and what are its primary uses? How can it be used in a backup strategy?**
* **What is disk striping, and how might it be considered the opposite of disk mirroring?**
* **Beyond simply identifying what to back up, when to back it up, and how to restore it, what should a complete backup recovery plan include?**
* **What is electronic vaulting, and how is it used in a backup strategy?**
* **What is remote journaling, and how is it used in a backup strategy?**
* **What is database shadowing?**
* **What is virtualization?**
* **Explain the shared-use strategies: time-share, service bureau, and mutual agreement.**
* **What are the phases of the overall IR development process?**
* **What are the general stages followed by the IRP team?**
* **Which individuals should be assembled to form the IRP team?**
* **What should be among the first deliverables created by the IR planning committee?**
* **What is the primary function of the IR Policy?**
* **What is an incident response plan (IR plan)?**
* **What characteristics must be present if an adverse event is to be considered an incident?**
* **What are the three sets of time-based procedures that are often part of the IR planning process?**
* **What is meant by the “trigger” for an IR-related plan?**
* **What is a “reaction force” in terms of IR planning?**
* **What is an after-action review (AAR)?**
* **What are the ways training can be undertaken for the CSIRT?**
* **Briefly describe the strategies used to test contingency plans?**
* **Briefly describe the possible training delivery methods?**
* **Provide a brief summary of the three main steps involved in contingency planning.**
* **What is an AAR, and why is it valuable to organizations? Which one of the three set of incident handling procedures is produced?**

**Short Answer / Essay Questions**.

**Compare between Business Impact Analysis (BIA) and Risk Management in term of dealing with security incidents.**

**Correct Answer:**

In risk management, all possible threats and vulnerabilities are identified and evaluated to propose countermeasures/controls to prevent possible attacks. On the other hand, BIA try to answer the question "If an attack succeed, what do you do next". This usually done through an investigation and assessment of the impact that various events or incidents can have on the organization.

**What are the primary responsibilities of the contingency planning management team (CPMT)?**

**Correct Answer:**

* Obtaining commitment and support from senior management
* Managing and conducting the overall CP process
* Writing the master CP document
* Conducting BIA
* Organizing and staffing the leadership of subordinate teams
* Providing guidance to and integrating the work of the subordinate teams.

**The circumstances that cause an IR team to be activated and an IR plan to be initiated are called triggers. Give three examples of possible IR triggers.**

**Correct Answer:**

* A phone call from a user to the help desk about unusual computer or network behavior Notification from a systems administrator about unusual server or network behavior Notification from an intrusion detection device
* Review of system log files indicating an unusual pattern of entries Loss of system connectivity
* Device malfunctions

**Explain the After-Action Review (AAR) process.**

**Correct Answer:**

Detailed examination of events

Key players review and verify notes, documentation Update plan and train future staff

**Can you outline the actions IR process phases?**

**Correct Answer:**

Preparation, detection and analysis, containment, eradication and recovery, and post- incident activity

**What are the possible indicators of an Incident?**

**Correct Answer:**

* Presence of unfamiliar files
* Presence or execution of unknown programs or processes
* Unusual consumption of computing resources
* Unusual system crashes

**Compare between RAID level 0, RAID level 1, RAID level 5 as a data recovery tools?**

**Correct Answer:**

**RAID 0: disk striping**

Does not give redundant storage media, it combines more than one disk (physical disks) to form a one larger logical disk.

**RAID 1: mirroring / duplexing**

In this type, each disk has a mirror, provide full data redundancy, if a disk become corrupted; data can be restored from mirror of the disk.

It can be considered the best solution for redundancy but it has high cost in comparison with other types.

it has two types based on controller type either control the disk and mirror ( mirroring ) or separate controller for the disk and another controller for the mirror ( duplexing )

**RAID 5:**

It is a balance between redundancy and cost, it support redundancy with balance in cost.

**Differentiate between full backup, incremental backup, differential backup and explain 6-tape backup strategy.**

**Correct Answer:**

**Full backup:** backup of all system files.

**Differential backup:** is the backup of all data/transactions after the last full backup.

**Incremental backup:** is the backup of data/transactions after the last incremental backup)

**6-tape strategy.**

In this strategy a tape is devoted for each day of week (tape for Sunday, tape for Monday ...etc ) , on Friday of first week we make the full backup on the 5th tape

We repeat the process for the second week but on next Friday, we use tape number 6.

And so on, in this strategy it is guaranteed that at any time we have a problem we can restore data from last full backup plus applying transaction from incremental backups.

**You are working as a Network Manager for Gulf News. As a network manager, you have to devise a backup strategy which will ensure that no data is lost and backup process takes less time with minimum hardware resources. Propose a backup strategy that can meet these requirements.**

**Correct Answer:**

Response should discuss the type of back up strategy that will be deployed. The response should be including different backup strategies such as Full Time Backup can be done once a week followed by differential backup done every day. Response should also include how the devise strategy meets the requirements of the end user.

**Describe Network-Attached Storage (NAS) and Storage Area Networks (SAN) then compare between them in terms of: connection and usage.**

**Correct Answer:**

•NAS uses single device or server attached to a network with common communications methods to provides online storage environment

–Good for general file sharing or data backup use

•SAN uses fiber-channel direct connections between systems needing additional storage and storage devices themselves

–Good for high-speed and higher-security solutions

**1. What are the NIST SP 800-34 Rev 1 seven steps of contingency planning?**

**Correct Answer:**

1. Develop the contingency planning policy statement

2. Conduct the business impact analysis

3. Identify preventative controls

4. Develop recovery strategies

5. Develop an information system contingency planning

6. Ensure plan testing, training, and exercises

7. Ensure plan maintenance

**2. What are the primary responsibilities of the contingency planning management team (CPMT)?**

**Correct Answer:**

CPMT responsibilities:

* 1. Obtain commitment and support
  2. Manage and conducting the overall CP process
  3. Write the master CP document
  4. Conduct the business impact analysis (BIA)
     + Assist in identifying and prioritizing threats and attacks
     + Assist in identifying and prioritizing business functions
  5. Organize and staff subordinate teams leadership
     + Incident response
     + Disaster recovery
     + Business continuity
     + Crisis management
  6. Provide guidance to and integrate the work of the subordinate teams

**Correct Answer: (Short)**

* Obtaining commitment and support from senior management
* Managing and conducting the overall CP process
* Writing the master CP document
* Conducting BIA
* Organizing and staffing the leadership of subordinate teams
* Providing guidance to and integrating the work of the subordinate teams.

**3. Describe Network-Attached Storage (NAS) and Storage Area Networks (SAN) then compare between them in terms of: Connectivity, File addressing, File identification, File transfer, OS support, File system management, and backups and mirrors.**

**Correct Answer:**

• NAS uses single device or server attached to a network with common communications methods to provides online storage environment

* Good for general file sharing or data backup use

• SAN uses fiber-channel direct connections between systems needing additional storage and storage devices themselves

* Good for high-speed and higher-security solutions

|  |  |  |
| --- | --- | --- |
|  | NAS | SAN |
| Connectivity | Any machine that can connect to a LAN and use standard protocols (such as NFS, CIFS, or HTTP) | Only server-class devices with SCSI fiber channel; a topology limit of 10 KM |
| Addressing, identification, and file transfer | By file name, with NAS handling security, including permissions, authentication, and file locking | By disk block number, with no individual security control |
| OS support | Greater sharing, especially between differing Oss | OS dependent and not compatible with all Oss |
| File system | Managed by NAS head unit | Managed by servers |
| Backups and mirrors | Done on files to save time and bandwidth | Done on blocks, requiring destination to be greater than source volumes |

**Correct Answer: (Short)**

•NAS uses single device or server attached to a network with common communications methods to provides online storage environment

–Good for general file sharing or data backup use

•SAN uses fiber-channel direct connections between systems needing additional storage and storage devices themselves

–Good for high-speed and higher-security solutions

**4. Compare between hot, warm, and cold sites as resumption strategies.**

**Correct Answer:**

**a. Hot site:** fully site equipped with software and hardware, this type have also data replication and can restore the business in a short notice, and it is the highest cost.

Fully configured computer facilities with all services, communications links, and physical plant operations

* + Can establish operations at a moment’s notice
* Can be staffed around the clock to transfer control almost instantaneously
  + Requires e-vaulting, RJ, or data shadowing
  + Disadvantages: most expensive alternative
  + Must provide maintenance for all systems, equipment
* Ultimate hot site: mirrored site identical to primary site

**b. Warm site:** partially equipped site with hardware, no software is installed or configured, this type of solution needs more time to restore business in comparison with hot site and has less cost.

* Provide similar services and options as a hot site
  + Software applications not included, installed, or configured
  + Frequently includes computing equipment and peripherals with servers; no client workstations
  + Has connections to facilitate quick data recovery
* Some advantages of a hot site, but at a lower cost
* May require hours, perhaps days for full functionality
* Customized costs
  + Range upward of several thousand dollars per month

**c. Cold site:** it is only space, with utilities services. Software and hardware are not installed. This is the cheapest solution but need more time to restore business.

Provide only rudimentary services and facilities

* + No computer hardware or peripherals provided
* All communication services must be installed after site occupied
* No quick recovery or data duplication functions
* Empty room with standard heating, air conditioning, and electrical service
* Advantages
  + Better than nothing; reduced contention for floor space
  + Cost: few thousand dollars per month

**Correct Answer: (Short)**

For site resumption strategies we have three options depend on cost.

**1. Hot site:** fully site equipped with software and hardware, this type have also data replication and can restore the business in a short notice, and it is the highest cost.

**2. Warm site:** partially equipped site with hardware, no software is installed or configured, this type of solution needs more time to restore business in comparison with hot site and has less cost.

**3. Cold site:** it is only space, with utilities services. Software and hardware are not installed. This is the cheapest solution but need more time to restore business.

**5. What is a redundant array of independent disks (RAID), and compare between RAID level 0, RAID level 1, RAID level 5 as a data recovery tools?**

**Correct Answer:**

**Redundant array of independent drives (RAID)**

* + Uses multiple hard drives to store information
  + Provides operational redundancy by spreading out data and using checksums
  + Does not address need for off-site storage

**RAID 0: disk striping**

Does not give redundant storage media, it combines more than one disk (physical disks) to form a one larger logical disk.

* + - Disk striping: Data segments written in turn to each disk drive in the array
    - Disk striping without parity: Occurs when multiple drives combined in order to gain large capacity without data redundancy
    - Increased risk: losing data from a single drive failure

**RAID 1: mirroring / duplexing**

In this type, each disk has a mirror, provide full data redundancy, if a disk become corrupted; data can be restored from mirror of the disk.

It can be considered the best solution for redundancy but it has high cost in comparison with other types.

it has two types based on controller type either control the disk and mirror ( mirroring ) or separate controller for the disk and another controller for the mirror ( duplexing ).

* + Disk mirroring
    - Uses twin drives in a computer system
    - Computer records data to both drives simultaneously
    - Provides a backup if the primary drive fails
    - Expensive and inefficient media use
    - Same drive controller manages both drives
  + Disk duplexing
    - Each drive has its own controller
    - Can create mirrors and splits disk pairs to create highly available copies of critical system drives

**RAID 5:**

It is a balance between redundancy and cost, it support redundancy with balance in cost.

* + Balances safety and redundancy
    - Against costs of acquiring and operating systems
  + Data segments interleaved with parity data
    - Written across all drives in the set
  + RAID 5 drives can be hot swapped
    - Replaced without taking entire system down

**6. Explain the shared-use strategies: time-share, service bureau, and mutual agreement.**

**Correct Answer:**

* **Time-share** 
  + Operates like hot/warm/cold site
  + Leased in conjunction with a business partner or sister organization
  + Provides DR/BC option while reducing overall cost
  + Disadvantages
    - Facility made be needed simultaneously
    - Need to stock facility with equipment and data from all involved organizations
    - Complex negotiating
    - Party may exit agreement or sublease their options
* **Service bureaus** 
  + Service agency that provides a service for a fee
  + Service in the case of DR/CP
    - Provision of physical facilities in the event of a disaster
  + Agencies frequently provide off-site data storage (fee)
  + Service bureaus contracts
    - Specify exactly what the organization needs under what circumstances; guarantees space when needed
  + Disadvantages
    - Expensive option
    - Must be renegotiated periodically
* **Mutual agreements** 
  + Contract between two organizations
    - Assist the other in the event of a disaster
    - Obligation to provide necessary facilities, resources, services until receiving organization recovers

**7. Evaluate the contingency planning to describe any five purpose of contingency planning policy.**

**Correct Answer:**

* **Purpose of policy**
  + Define the CP operations scope
  + Establish managerial intent with regard to timetables for incident response
  + Recovery from disasters
  + Reestablishment of operations for continuity
  + Establish responsibility for the development and operations of the CPMT in general
  + Provide specifics on CP-related team constituencies

**8. What is remote journaling, and how is it used in a backup strategy?**

**Correct Answer:**

* Transfers live transactions to an off-site facility
* Only transactions transferred (not archived data)
* Transfer performed online; much closer to real time
* Involves online activities on a systems level
  + Data written to two locations simultaneously
  + Can be performed asynchronously
* Facilitates key transaction recovery in near real time
* Journaling may be enabled for an object
  + Operating system creates record of object’s behavior
  + Stored in a journal receiver

**9. Differentiate between full backup, incremental backup, differential backup and explain 6-tape backup strategy.**

**Correct Answer:**

**Full backup:** backup of all system files.

**Differential backup:** is the backup of all data/transactions after the last full backup.

**Incremental backup:** is the backup of data/transactions after the last incremental backup)

**6-tape strategy.**

In this strategy a tape is devoted for each day of week (tape for Sunday, tape for Monday ...etc ) , on Friday of first week we make the full backup on the 5th tape

We repeat the process for the second week but on next Friday, we use tape number 6.

And so on, in this strategy it is guaranteed that at any time we have a problem we can restore data from last full backup plus applying transaction from incremental backups.

**10. Define what is risk management and explain its sub processes. What is the relationship between risk management and BIA?**

**Risk management:** is the process of identifying risks threatening the organization, assessing these risks, and selecting the suitable control strategy to mitigate or prevent this risk.

* + - * **Risk identification process:** is e examining, documenting, and assessing the security posture of an organization’s IT and the risks it faces.
      * **Risk assessment:** is the process of calculating risk for each vulnerability to get more details and knowledge about risk, the risk assessment will give a score for each vulnerability which makes comparison easier and contingency planner can decide what is the most dangerous threat threatening the organization.
      * **Risk control process:** selecting and applying the most appropriate control to mitigate the risk.

The most important sub process is risk assessment, as it is an input source for BIA analysis.

**11. Refer to the below analysis weighted factor worksheet and answer the questions.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset** | **Impact on Revenue (40)** | **Impact on Profitability (20)** | **Impact on Public Image (40)** | **Result** |
| **Mail Server** | **0.2** | **0.4** | **0.7** |  |
| **Web Server** | **0.1** | **0.5** | **0.6** |  |
| **Application Server** | **0.8** | **0.7** | **0.5** |  |

**1- Calculate the weight value of each asset and show your work.**

**2- Which asset is the most important asset based on your results in step 1 above?**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset** | **Impact on Revenue (40)** | **Impact on Profitability (20)** | **Impact on Public Image (40)** | **Result** |
| **Mail Server** | **0.2** | **0.4** | **0.7** | **44** |
| **Web Server** | **0.1** | **0.5** | **0.6** | **38** |
| **Application Server** | **0.8** | **0.7** | **0.5** | **66** |

**Mail Server = 0.2 \* 40 + 0.4 \* 20 + 0.7 \* 40 = 44**

**Web Server = 0.1 \* 40 + 0.5 \* 20 + 0.6 \* 40 = 38**

**Application Server = 0.8 \* 40 + 0.7 \* 20 + 0.5 \* 40 = 66**

**- Application server is the most valuable asset in the list.**

**12. Explain the difference are between DRP and BCP, why they are combined under BRP name?**

**DRP**

* Preparations for the recovery process
* Strategies to limit losses during the disaster
* Detailed steps to follow after the immediate danger

**BCP**

* Expresses how to ensure critical business functions continue at an alternate location
* After a catastrophic incident or disaster
* Used when DRP cannot restore primary site operations
* Most strategic and long-term plan

**BCP and DRP are usually combined together under BRP for many reasons:-**

**-** They overlapped in time, usually activated together.

- Teams of both plans work together

- Budgetary planning usually combined

**13.**

**a) An organization need to replicate a database in remote locations, across a public or private carrier. Demonstrate three different replication types that can be used for the backup.**

**b) Choose a suitable data replication solution for your organization and justify your selection.**

Three types of Database replication

1. Snapshot replication- copying data from one DB to another
2. Merger replication-merging data from multiple DBs into separate one.
3. Transaction replication-master DB for regular operations, but periodically copy new and updates to a backup

I will select database shadowing because it writes multiple database copies simultaneously in two separate locations, which is better than remote journaling or electronic valuating.

**14. The circumstances that cause an IR team to be activated and an IR plan to be initiated are called triggers. Demonstrate three examples of possible IR triggers.**

Any three points:

1. A phone call from a user to the help desk about unusual computer or network behavior

2. Notification from a systems administrator about unusual server or network behavior

3. Notification from an intrusion detection device

4. Review of system log files indicating an unusual pattern of entries

5. Loss of system connectivity

6. Device malfunctions

**15. During a routine system check, you as an IR member, have identified malware is running on a system. What the necessary steps that you will follow in the response to your findings, list 6 steps.**

1. Verify virus presence

2. Confirm presence and determine extent of exposure

3. Quarantine infestation

4. Disconnect infected systems from network and Look for evidence of continued spread

5. Continue to look for “flare-ups”

6. Begin the next phase: decontamination

7. Isolate infected computers

8. Clean infected computers from the malware

9. Recover deleted/corrupted files

10. Reconnect computers and keep monitoring

**16. Policy governing incident response is highly individualized to the organization. However, most policies include the same key elements: list three elements?**

* Statement of management commitment
* Purpose and objectives of the policy
* Scope of the policy (to whom and what it applies and under what circumstances)
* Definition of computer security incidents
* Organizational structure and delineation of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, and the requirements and guidelines for external communications and information sharing
* Prioritization or severity ratings of incidents
* Performance measures
* Reporting and contact forms

**17.**

**a) Discuss the difference between IDS and IDPS.**

**b) Discuss their placement in the network and.**

**c) Discuss their detection approaches.**

**a) The main difference between IDS and IDPS is:**

**IDS: intrusion detection system can only detect the incident while IDPS and detect and prevent the incident.**

**b) Placement in network:**

**1. Inline sensor: in this type sensor is put behind the firewall, all traffic pass through the sensor, and sensor can check the traffic and report to NIDPS.**

**2. Passive sensor: set outside of a network segment and connected through the SPAN port to this segment, it can monitor all the traffic and report to NIDPS.**

**c) Detection approaches:**

**1. Signature-based IDPS: in this way traffic is checked against patterns matching known signatures**

**2. Anomaly-based IDPS: here traffic is checked and compared to base line called clipping level.**

**18. Explain IR Response strategies for malware outbreaks.**

1. Filtering e-mail based on subject, attachment type using malware signatures, or other criteria

2. Blocking known attackers (block known attacker addresses)

3. Interrupting some services (mail servers until updating of virus database patterns)

4. Disconnect networks from the Internet or each other

5. Engaging the users - training

6. Disrupting service may disrupt malware vectors.

**19.**

**a) Discuss the false negative and false positive alarms and how they can affect incident detection.**

**b) What does the term “tuning” mean with respect to an IDPS?**

**A**

**1) False Positive**: Normal User Traffic is processed by IPS and alarm is falsely generated. We need to tune the IDS by turning this to True Negative.

**2) False Negative:** Attack traffic is processed by IPS but no alarm generated. We need to tune the IDS and turn this to True Positive.

**B**

* Tuning is related to the change of IDPS settings or configurations. The network manager has to change the settings and configuration to stop any new threats.
* Tuning is change in configuration to minimize both false positive and false negative.

**20. What are the possible indicators of an Incident?  List 4 of them.**

* + - 1. Presence of unfamiliar files
      2. Presence or execution of unknown programs or processes
      3. Unusual consumption of computing resources
      4. Unusual system crashes

**21. How can you prepare to protect your system from unauthorized access incidents?**

* Placing a common central log server in a more highly protected area of the network will certainly assist in post-event analyses
* Implementing an effective password policy and having both a complete and usable management policy
* as well as technology-enforced password requirements is critical

**22. Assume an organization that has different branches across the country with a headquarter in Dubai, Discuss the needed CSIRT structural category for this organization.**

Due to the distributed nature of the organization, incidents may occur at any location of the organizations. Therefore, it is recommended to have a Distributed CSIRTs structural category, which includes multiple CSIRTs to handle incidents at their physical segments.

**23. The organization XYZ has encountered an attack and it left some damages. This incident has also charged the organization extra costs. list the steps that the organization should consider in determining the cost with an associated incident.**

* Cost associated with the number of person-hours diverted from normal operations to react to the incident.
* Cost associated with the number of person-hours needed to recover data.
* Opportunity costs associated with the number of person-hours that could have been devoted to working on more productive tasks.

**24. Develop the proper incident handling strategy for an "Inappropriate use incident" to handle the incident during its occurrences of an organization that does not have a proper policy? And Advise accordingly on the proper step to be taken to prevent such incident from reoccurring?**

During the IU incident: The organization should clearly define the circumstances under which the CSIRT and/or management may investigate the interior of a piece of organization equipment.

Prevention is actually the handling of the IU incident Before it occurs which require a proper policy to be in place and this policy must be enforceable through Dissemination (distribution), Review (reading), Comprehension (understanding), Compliance (agreement) and Uniform enforcement.

**25. What are inline sensors and passive sensors in IDPS? Where the inline sensors and passive sensors are placed in a network?**

Inline and passive sensor both are network-based placement for IDPS

Inline sensor: monitor the live traffic pass in and out, to detect and prevent the attack in real time, Placed: inside the firewall

Passive sensor: captured the traffic in and out, store them to analyze them later (ex: sport, mirror port), Placed: next to the network (separated).

**26. Discuss the IR tasks to be performed before and during DDoS attack.**

**Before DDoS:**

- Preparation

- Prevention (controls)

- coordinate with internet service provider (ISP)

- make a log file and documentation (backup/store)

- monitor the resources

**During DDoS:**

- Find the target system, host

- fix the source of the problem

- filter the attacker

- disable connection for the compromised system

- Temporarily shutdown

**27. Highlight the difference between Signatures based detection and Anomaly based detection approaches in IDPS**

**Signature based:** (knowledge based) store the bad packets (ubnormal) , if there is a match the alarm will rise, need to update from time to time.

**Anomaly based:** (behavior based) store the good behavior (normal uses), if there is changes in the normal uses (not match) the alarm will rise.

**Signature-based IDPS (knowledge-based)**

Examines data traffic in search of patterns matching known signatures

Weaknesses:

* Signatures must be continually updated
* Time frame over which attacks occur

**Anomaly-based IDPS (behavior-based IDPS)**

Samples network activity and applies statistical analysis against a baseline

Clipping level: Measured activity outside baseline parameters

**28. What are the seven-step DRP process recommended by NIST?**

1. Develop the DR planning policy statement
2. Review the business impact analysis (BIA)
3. Identify preventive controls
4. Create DR contingency strategies
5. Develop the DR plan
6. Ensure DR plan testing, training, and exercises
7. Ensure DR plan maintenance

**29. List the primary DR team representatives?**

* 1. Senior management
  2. Corporate support
  3. Facilities
  4. Fire and safety
  5. Maintenance staff
  6. IT technical staff
  7. IT managers
  8. InfoSec technicians
  9. InfoSec managers

**30. Compare between Business Impact Analysis (BIA) and Risk Management in term of dealing with security incidents.**

**Correct Answer:**

In risk management, all possible threats and vulnerabilities are identified and evaluated to propose countermeasures/controls to prevent possible attacks. On the other hand, BIA try to answer the question "If an attack succeed, what do you do next". This usually done through an investigation and assessment of the impact that various events or incidents can have on the organization.

**31. What are the primary responsibilities of the contingency planning management team (CPMT)?**

**Correct Answer:**

* Obtaining commitment and support from senior management
* Managing and conducting the overall CP process
* Writing the master CP document
* Conducting BIA
* Organizing and staffing the leadership of subordinate teams
* Providing guidance to and integrating the work of the subordinate teams.

**32. The circumstances that cause an IR team to be activated and an IR plan to be initiated are called triggers. Give three examples of possible IR triggers.**

**Correct Answer:**

* A phone call from a user to the help desk about unusual computer or network behavior Notification from a systems administrator about unusual server or network behavior Notification from an intrusion detection device
* Review of system log files indicating an unusual pattern of entries Loss of system connectivity
* Device malfunctions

**33. Explain the After-Action Review (AAR) process.**

**Correct Answer:**

* Detailed examination of events.
* Key players review and verify notes, documentation Update plan and train future staff.

**34. Policy governing incident response is highly individualized to the organization. However, most policies include the same key elements: list three elements?**

**Correct Answer:**

* Statement of management commitment Purpose and objectives of the policy
* Scope of the policy (to whom and what it applies and under what circumstances) Definition of computer security incidents
* Organizational structure and delineation of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, and the requirements and guidelines for external communications and information sharing
* Prioritization or severity ratings of incidents Performance measures
* Reporting and contact forms

**35. Can you outline the actions IR process phases?**

**Correct Answer:**

Preparation, detection and analysis, containment, eradication and recovery, and post- incident activity

**36. What are the possible indicators of an Incident?**

**Correct Answer:**

* Presence of unfamiliar files
* Presence or execution of unknown programs or processes
* Unusual consumption of computing resources
* Unusual system crashes

**37. What is the difference between IDS and IPS?**

**Correct Answer:**

**- Intrusion detection systems (IDSs)**

Detects a violation and activates an alarm

Custom configuration levels available

**- Intrusion prevention system (IPS)**

Detects intrusion and prevents successful attack using an active response

**38. The services of a CSIRT can be grouped into which three categories?**

**Correct Answer:**

* Reactive services
* Proactive services
* Security quality management services

**39. What are the disaster classifications?**

**Correct Answer:**

* Man-made disasters.
* Rapid-onset disasters.
* Slow-onset disasters

**40. When disaster occurs organizations need to?**

**Correct Answer:**

* Meticulous preparation and ongoing diligence
* Quick and decisive reaction to restore operations
* To prepare to promptly reestablish operations at a new permanent location

**41. The primary DR team includes representatives from different departments. Mention 4 of these departments?**

**Correct Answer:**

* Senior management
* Corporate support
* Facilities
* Fire and safety
* Maintenance staff
* IT technical staff
* IT managers
* InfoSec technicians
* InfoSec managers

**43. Differentiate between full backup, incremental backup, differential backup and explain 6-tape backup strategy.**

**Correct Answer:**

**Full backup:** backup of all system files.

**Differential backup:** is the backup of all data/transactions after the last full backup.

**Incremental backup:** is the backup of data/transactions after the last incremental backup)

**6-tape strategy.**

In this strategy a tape is devoted for each day of week (tape for Sunday, tape for Monday ...etc ) , on Friday of first week we make the full backup on the 5th tape

We repeat the process for the second week but on next Friday, we use tape number 6.

And so on, in this strategy it is guaranteed that at any time we have a problem we can restore data from last full backup plus applying transaction from incremental backups.

**44. You are working as a Network Manager for Gulf News. As a network manager, you have to devise a backup strategy which will ensure that no data is lost and backup process takes less time with minimum hardware resources. Propose a backup strategy that can meet these requirements.**

**Correct Answer:**

Response should discuss the type of back up strategy that will be deployed. The response should be including different backup strategies such as Full Time Backup can be done once a week followed by differential backup done every day. Response should also include how the devise strategy meets the requirements of the end user.

**45. Describe Network-Attached Storage (NAS) and Storage Area Networks (SAN) then compare between them in terms of: connection and usage.**

**Correct Answer:**

•NAS uses single device or server attached to a network with common communications methods to provides online storage environment

–Good for general file sharing or data backup use

•SAN uses fiber-channel direct connections between systems needing additional storage and storage devices themselves

–Good for high-speed and higher-security solutions

**46. Compare between hot, warm, and cold sites as resumption strategies.**

**Correct Answer:**

For site resumption strategies we have three options depend on cost.

1. Hot site: fully site equipped with software and hardware, this type have also data replication and can restore the business in a short notice, and it is the highest cost.

2. Warm site: partially equipped site with hardware, no software is installed or configured, this type of solution needs more time to restore business in comparison with hot site and has less cost.

3. Cold site: it is only space, with utilities services. Software and hardware are not installed. This is the cheapest solution but need more time to restore business.

**47. Sketch the use of Host based NIDPS and illustrate its placement.**

**Correct Answer:**

* Resides on a particular computer or server (host)
* Monitors activity on that system
* Alert or alarm triggers
* File attributes change, new files created, existing files deleted
* Can monitor systems logs for predefined events
* HIDPS log file provides an independent audit trail
* Very reliable
* False positive alert produced only when authorized monitored file changed
* Can access encrypted information
* Information to determine legitimate traffic present

**48. Compare and contrast between rapid onset disaster and slow onset disaster.**

**Correct Answer:**

**Rapid-onset disasters**

Those that occur suddenly, with little warning, taking the lives of people and destroying the means of production

**Slow-onset disasters**

Occur over time and slowly deteriorate the organization’s capacity to withstand their effects

**(Students can give reasonable examples)**

**49. Illustrate the primary goals of Disaster Recovery- Recovery phase.**

**Correct Answer:**

* Primary goals of the recovery phase
* Recover critical business functions
* Coordinate recovery efforts
* Acquire resources to replace damaged or destroyed materials and equipment
* Evaluate the need to implement the BC plan.

**50. Apply your knowledge to build the Computer Security Incident Response Team (CSIRT) at your organization, show how do you select members for the team, what kind of structure you will use and what staffing model, and describe nontechnical skills needed for the team.**

* Selection members of the team depend on the background of the IR team, all members within formation technology background or information security background will be the members of this team
* Structure of the team depends on the organization if it has one branch or more, so in case of one branch organization I will select to use centralized CSIRT, and If the organization has many branches I will use the distributed CSIRT
* Staffing, either I will use fully employee CSIRT or partially outsourcing team
* Nontechnical skills needed: communication, coordination, writing, oral presentation skills.

**51.**

**a) An organization need to replicate a database in remote locations, across a public or private carrier. Demonstrate three different replication types that can be used for the backup.**

**b) Choose a suitable data replication solution for your organization and justify your selection.**

a) –Three types of Database replication:

* Snapshot replication- copying data from one DB to another
* Merger replication-merging data from multiple DBs into separate one
* Transaction replication-master db for regular operations, but periodically copy new and updates to a backup

b) I will select database shadowing because it writes multiple database copies simultaneously in two separate locations which is better than remote journaling or electronic valulting.

**52. Assume an organization, with a limited budget, adopts the hot site exclusive site resumption strategy during the process of preparation for the organization's DRP. Produce a defending statement to show that this strategy is not suitable for them.**

Hot sites assume having the following:

1. A fully configured computer facilities with all services and communications links, with the latest data backups strategies

2. Staffed around the clock to transfer control almost instantaneously

as a result to the above, Adopting the hot site strategy requires careful consideration to the specific business needs along with the costs and the needed capabilities especially when creating a site that is identical to primary site with live or periodic data transfer.

**53. The circumstances that cause an IR team to be activated and an IR plan to be initiated are called triggers. Demonstrate three examples of possible IR triggers.**

1. A phone call from a user to the help desk about unusual computer or network behavior
2. Notification from a systems administrator about unusual server or network behavior
3. Notification from an intrusion detection device
4. Review of system log files indicating an unusual pattern of entries
5. Loss of system connectivity
6. Device malfunctions

**54. During a routine system check, you as an IR member, have identified malware is running on a system. What the necessary steps that you will follow in the response to your findings, list 6 steps.**

1. Verify virus presence
2. Confirm presence and determine extent of exposure
3. Quarantine infestation
4. Disconnect infected systems from network and Look for evidence of continued spread
5. Continue to look for “flare-ups”
6. Begin the next phase: decontamination
7. Isolate infected computers
8. Clean infected computers from the malware
9. recover deleted/corrupted files
10. reconnect computers and keep monitoring

**55. Salem is a backup operator. He takes full backup of database server on every Friday. For rest of the week, he is taking differential back up every morning at 3 AM. On Tuesday morning database server crashed because of an unexpected power failure. Write down the recovery procedure for given situation to help Omar to recover the database?**

A differential backup type includes all files changed or added since full backup. Salem should perform the following steps:

1 - Restore the full backup that he has taken on last Friday.

2 – Restore the last differential backup that he has taken on Tuesday night at 3 AM.

**56. There are a number of organizational models that a CSIRT can follow. Some considerations for how a CSIRT may be structured include a need for coverage, availability of employees, and cost. Assume an organization that has different branches across the country with a headquarter in Dubai, Discuss the needed CSIRT structural category for this organization**

Due to the distributed nature of the organization, incidents may occur at any location of the organizations. Therefore, it is recommended to have a Distributed CSIRTs structural category which includes multiple CSIRTs to handle incidents at their physical segments.

**57. Construct three different feedback mechanism options to evaluate the CSIRT effectiveness.**

- Compare local CSIRT measures to other CSIRTs

- Solicit comments from CSIRT’s constituency

- Use periodic surveys to gain insight from a constituency

- Collect, report, and audit a set of empirical measures

**58. The organization XYZ has encountered an attack and it left some damages. This incident has also charged the organization extra costs. List the steps that the organization should consider in determining the cost with an associated incident.**

* Cost associated with the number of person-hours diverted from normal operations to react to the incident
* Cost associated with the number of person-hours needed to recover data
* Opportunity costs associated with the number of person-hours that could have been devoted to working on more productive tasks

**59. Develop the proper incident handling strategy for an "Inappropriate use incident" to handle the incident during its occurrences of an organization that does not have a proper policy? and Advise accordingly on the proper step to be taken to prevent such incident from reoccurring?**

During the IU incident the organization should clearly de􀃑ne the circumstances under which the CSIRT and/or management may investigate the interior of a piece of organization equipment.

Prevention is actually the handling of the IU incident before it occurs which require a proper policy to be in place and this policy must be enforceable through:

1. Dissemination (distribution),
2. Review (reading),
3. Comprehension (understanding),
4. Compliance (agreement) and
5. Uniform enforcement.

**60. What makes an organization ready to respond to disasters?**

* Meticulous preparation and ongoing diligence
* Quick and decisive reaction to restore operations
* To prepare to promptly reestablish operations at a new permanent location

**61. The principal objective of the disaster recovery policy is to develop, test and document a well-structured and easily understood plan which will help the organization recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Explain in detail 4 elements that should appear in the Disaster Recovery Policy statement.**

* **Purpose:** provide and guidance of all DR operations.
* **Scope:** defense which organization unit to which this policy applies.
* **Roles and responsibilities:** This section identifies the roles and responsibilities of the key players in DR operations.
* **Resource requirements:** resources needed for development of DR plans.
* **Training requirements:** training for various types of employee categories are defined and highlighted
* **Exercise and testing schedules:** type of exercises and testing and who is involved.
* **Plan maintenance schedule:** frequency of plan maintenance and who is involved and instruction of update.
* **Special considerations:** any additional context not covered above may be added in this section

**62. Testing is critical to change management in disaster recovery planning. From this standpoint, testing helps to identify "gaps" in the recovery capability that you have developed to respond to a disruptive event and to assure continuous or near-continuous business operations. Explain 4 rehearsal and testing strategies that an organization can employ, and explain why it is essential to the organizing.**

**Rehearsal and testing strategies**

– Desk check

– Structured walk-through

– Simulation

– Parallel testing

– Full-interruption

– War gaming

The more important value of DR testing is rehearsal. The more you can rehearse, the better your team members will understand their individual roles and the interdependencies between what they are doing and what others are doing. That is very important since it enables the teams to work in a mostly independent way and to perform tasks in a reasonably dependable way even in the face of a great irrationality -- a disaster.

**63. Disaster recovery planning enables you to prepare for a wide scope of natural and unnatural events that can threaten your business infrastructure and therefore your business operations. A disaster recovery plan (DRP) is a document that outlines the process or set of procedures used to recover and protect your business in the event of a disaster. The more comprehensive your DRP the better chance you have of returning to normal business promptly. Design an effective disaster recovery plan using five phase strategy.**

**Five phases of disaster recovery plan:**

**1. Preparation:** No prevention phase in DR planning

**2. Response:** Associated with implementing initial reaction to a disaster

**3. Recovery:** Recovery of the most time-critical business functions

**4. Resumption:** Focuses on non-critical functions

**5. Restoration:** begins once all damage assessments accomplished and Rebuilding of primary site has commenced

**64. Clearing subordinate activities are conducted when returning to the primary site after the DRP is completed. Describe why this step is necessary to the organization and how it is implemented?**

**The organization clear subordinate activities to:**

* Save in the cost
* Return the business in the primary site.
* Utilize all backups or equipment from the secondary site to the primary site.
* Discontinue with any leasing contract or SLA with providers.

**Implementation:**

* Redirecting employees back to normal work offices
* Scheduling of employee move: Not all business functions may return at the same time
* Disconnecting services Breakdown of equipment
* Packing up supplies, materials, and equipment and putting it in storage or transporting it to primary site
* Transferring building to BC service provider and clearing the building

**65. Develop a plan with at least 5 steps that are required when relocating to an alternate site.**

1. The official beginning of actual BC operations
2. The plan should specify conditions and how the organization relocates
3. Notify all necessary service providers (power, water, gas, telephone, Internet) and the BC site/alternate location owner
4. Notification of BC team to move to BC site/alternate location
5. Acquisition of supplies, materials, and equipment
6. Notification of employees to relocate to BC site/alternate location

**66. As a contingency planner at your organization, you have been asked to develop a business continuity team, describe how you build this team and describe its structure.**

* BC Team Leader and
* Specialists from CPMT
* Representatives from the IT Department and Information Security Department

**67. Your company faced a disaster that continued for 2 days , Explain any 3 key challenges faced during and after the disaster?**

• Widespread disasters frequently affect:

– Departments and various organization levels

– Communities encompassing the organization

– Vendors and suppliers

• Outside help may be unavailable for days or weeks

– Emergency services, public services, grocers and other suppliers, utility services, private services, telecommunications services, and air and surface transportation

• Worst-case scenario

– Seemingly routine event quickly spins out of control

• Most disaster-related losses cause:

– Inability to react properly to the disaster

– A need to improvise, adapt, and overcome obstacles

**Good Luck**