ISACA CISM - Quiz Questions with Answers

Incident Management

1.

An organization has decided to conduct an exercise in which they write their roles and duties on paper, determine how effective it is, and identify where they can improve based upon a given scenario. What type of exercise does this **BEST** describe?

Structured walkthrough

Checklist

Diagramming

Simulation test

Correct answer: Structured walkthrough

In a structured walkthrough, employees write their roles and duties on paper, determine how effective it is for a disaster recovery situation, and identify where they can improve based upon a given scenario. This allows for knowledge sharing, providing and receiving feedback, and ultimately results in a stronger disaster recovery team without major interruptions to the organization.

A checklist is more simplified, in which each individual is essentially given a list of their roles. A simulation test is dynamic and extremely beneficial to a workplace because it gives employees hands-on training within their role. However, a simulation can be time-consuming and disrupt normal business workflows. Diagramming is a fabricated term.

2.

Which of the following refers to the maximum period after an incident that critical operations/processes can be down before the company runs the risk of going out of business?

AIW

RTO

RPO

SDO

Correct answer: AIW

The acceptable interruption window (AIW) is the maximum period after an incident that critical services/processes can be down before the company runs the risk of going out of business.

The recovery point objective (RPO) measures how much data is lost after an incident. It is typically the age of the last known backup.

The recovery time objective (RTO) measures the maximum time until a process operates at an acceptable level before the business begins experiencing unacceptable impacts (financial, reputational, etc.).

The service delivery objective (SDO) refers to the level of service provided while the organization is resolving an incident with the main service.

3.

If the Incident Management Team (IMT) evaluates the computing infrastructure by using a security assessment tool, they are in what phase of the incident response lifecycle?

Protect

Respond

Detect

Triage

Correct answer: Protect

In the protect phase, actions are taken to reduce the likelihood of an attack and the impact if it does happen.

The respond phase is the actions taken to address, resolve, or mitigate an incident. The detect phase is where the Intrusion Detection System (IDS) sends a log, or when a user forwards an email, calls the help desk about a topic, etc. Triage is the prioritization of incidents so that they are assigned to the Incident Management Team (IMT) in an appropriate order.

4.

Which of the following is **LEAST** likely to be an incident management responsibility that an organization should consider?

Preparing employees to the level of first responders

Legal issues

Always being ready

Notifying necessary people

Correct answer: Preparing employees to the level of first responders

An organization is least likely to be responsible for training employees to the level of first responders. While basic first aid and CPR is important, going beyond that is unnecessary and may have a negative return on investment.

In any incident, an organization should consider legal issues, always be ready and prepared for an incident, and notify the appropriate people and have a call list.

5.

With recovery test metrics, which of the following describes the time from one failure to the next?

MTBF

MTTF

ARO

EF

Correct answer: MTBF

Mean time between failures (MTBF) is the average time between failures based upon multiple compared instances.

Mean time to failure (MTTF) is the average time it will take for an initial failure. Annual rate of occurrence (ARO) is how often something occurs in a year — you can use this measurement to determine the risk associated with repeated threats in a year, for example. The exposure factor (EF) of an asset is the percentage of that asset's value at risk.

6.

A corporation has determined that they cannot tolerate the loss of any transaction that has been committed to their sales database. Therefore, they can only tolerate losing a transaction that is in process. This is approximately 24 microseconds of tolerable loss.

What have they determined?

- **Recovery Point Objective (RPO)**
- Maximum Tolerable Outage (MTO)
- Recovery Time Objective (RTO)
- Service Delivery Objective (SDO)

Correct answer: Recovery Point Objective (RPO)

The RPO is the age of the data that must be restored after a failure, or the time worth of data that can be lost.

The MTO is the total time that the business can be at the alternate site. The RTO is the time to recover, whether it is from failure to function or declaration of disaster to functionality. Neither is the topic of the question, so whichever definition you prefer does not make a difference in terms of answering this question. The SDO is the percentage of functionality at the alternate site, such as 80% of the normal number of calls/connections from customers per hour.

7.

As a Disaster Recovery Plan (DRP) is being built for a corporation, the team will move through different phases. As the team moves from identifying a recovery strategy to developing the response and recovery plan, it is **ESSENTIAL** to:

Obtain management support

Research legal requirements

Communicate with shareholders

Enlist auditor support

Correct answer: Obtain management support

After a strategy is identified, the plan must be built. Building the alternate facilities, or whatever has been strategized, will usually cost a fair amount of money. It is essential to ensure that you have management support for the plan.

Legal requirements should have been researched before any strategies were created. Communication with shareholders will probably occur after the plan is developed rather than before. As there is no plan yet, just a strategy, auditor involvement of any kind is unlikely.

8.

Which of the following is the **BEST** example of a technical threat?

Abnormally hot servers due to HVAC failure

Emerging threats in cybersecurity

Shoulder surfing

Hurricanes

Correct answer: Abnormally hot servers due to HVAC failure

Abnormally hot servers due to an HVAC failure would be a technical threat, since it is the result of a technical device failing.

Emerging threats in cybersecurity refer to technical threats that involve technology. Shoulder surfing is a human threat, as it involves human interaction and direct human control. Abnormally hot servers due to an HVAC failure would be a technical threat, since it is the result of a technical device failing. A hurricane is an environmental threat.

9.

You are working on Business Continuity Planning (BCP) as the information security manager for a real estate company. You are currently looking into the availability needs of customer data.

Which of the following technologies has the **HIGHEST** availability?

- **Storage Area Network (SAN)**
- Network Attached Storage (NAS)
- Direct Attached Storage (DAS)
- Solid State Drive (SSD)

Correct answer: Storage Area Network (SAN)

A Storage Area Network (SAN) is a high-speed network that allows faster access to data. It also supports disk mirroring, backups, as well as many other features.

A Network Attached Storage (NAS) is attached to the existing Local Area Network (LAN), which is probably Ethernet. It is reasonably reliable but does not have all of the features of a SAN. Direct Attached Storage (DAS) is storage attached to the server or end station directly. It can be accessible from the network depending on the use of that end station. A Solid State Drive (SSD) is a type of drive that replaces magnetic media. It is more reliable, but for managing customer data within a business, the SAN is the critical technology that is needed.

10.

While doing their annual risk assessment for Business Continuity Planning (BCP), a research firm determined that they could tolerate losing four hours of their data. More than four hours would cause a great deal of damage to their business.

What have they defined?

- **Recovery Point Objective (RPO)**
- Recovery Time Objective (RTO)
- Maximum Tolerable Downtime (MTD)
- Service Delivery Objective (SDO)

Correct answer: Recovery Point Objective (RPO)

The Recovery Point Objective (RPO) defines the maximum acceptable amount of data loss measured in time. It represents how far back in time a business can go to recover data after a disruption without significant impact. For example, if the RPO is four hours, the organization can lose up to four hours' worth of data without severe consequences.

The Recovery Time Objective (RTO) is the time it takes for a service or system to be restored after an interruption.

Maximum Tolerable Downtime (MTD) refers to the maximum amount of time a business process can be inoperative without causing significant damage.

The Service Delivery Objective (SDO) is the level of functionality a system must achieve to operate adequately after recovery.

11.

When identifying important assets, what criteria would be of **LEAST** importance for an organization to take into consideration?

Asset popularity in the industry

Effect on overall operations

Dependencies

Ability to work around the issue

Correct answer: Asset popularity in the industry

Asset popularity in the industry is least important for an organization — what works for their business may not work for others, but fits their needs perfectly. Any organization has to consider the fact that new equipment means retraining employees to proficiency, which is risky and can impede business when unneeded.

What does matter is how the assets impact operations, what is dependent on the assets in question, and how the workplace utilizes resources and works around the issue of not using the most popular assets.

12.

Which of the following is **LEAST** likely to be covered by insurance?

A company decides not to encrypt data to follow GDPR in an effort to avoid key management, resulting in a breach

An employee of a company mistakenly releases customer data

Enterprise equipment is damaged after a water pipe breaks

An ex-employee reveals classified information

Correct answer: A company decides not to encrypt data to follow GDPR in an effort to avoid key management, resulting in a breach

A company that decides not to encrypt data that must be encrypted by regulation and subsequently is breached would not be covered by insurance. This is because it was wilfully negligent, not an accident.

An employee making an honest mistake would likely be covered by insurance. Company assets being damaged by disasters or accidents would also be covered, along with ex-employees releasing information maliciously.

13.

Paalavi has been working with the telecom and data provider to ensure that a backhoe cannot dig up all of the cables that provide access to their Wide Area Network (WAN). What has he been working on?

Last-mile protection

Voice recovery

Alternative routing

Redundancy

Correct answer: Last-mile protection

The best answer here is last-mile protection.

In protecting that last mile, redundancy is added, but in this context, redundancy would be considered within the network. Alternative routing is a possible answer, but the situation does not involve a different medium, such as dial-up, cellular, microwave, fiber vs. cable, etc. Voice recovery is close in that it ensures that the telecoms continue to work, but again, the better answer is last-mile protection because of the very specific scenario.

14.

Which of the core goals of an incident management strategy is the **HARDEST** to achieve?

Eliminating threats

Mitigating threats

Reducing threat likelihood

Reducing potential threat impacts

Correct answer: Eliminating threats

The three core elements of an incident management strategy are eliminating or neutralizing threats, minimizing the likelihood of a threat, and minimizing a threat's potential impacts. Eliminating threats is the hardest goal to achieve because it may be impossible to do so.

Mitigating threats is an umbrella term that covers both reducing the likelihood of a threat and minimizing a threat's potential impacts.

15.

Harris and his team have been working to determine critical systems, their interdependencies, possible disruptions, and providing information on possible restoration methods. What have they been doing?

A Business Impact Analysis (BIA)

A gap analysis

A formal audit/assessment

A risk assessment

Correct answer: A Business Impact Analysis (BIA)

The question covers the basics of a BIA.

A gap analysis is when you look for the difference between or distance from where you are in comparison to where you want to be. A formal audit involves someone coming in from the outside world. The question does not state or imply that this is true. Additionally, an audit looks to see if things are being done according to a standard, framework, policy, etc. A risk assessment does look at critical systems and what can happen, but not at possible restoration methods, making it incorrect.

16.

Which of the following is the greatest metric to determine the likelihood of an attempted breach of a public-facing web server?

Ten failed authentication attempts in ten minutes

Three ping sweeps in the past day

Vulnerability scan results

A CVSS score of 2.1

Correct answer: Ten failed authentication attempts in ten minutes

Ten failed authentication attempts in ten minutes is a clear metric that there is some risk of a breach. This is a prime example of a key risk indicator (KRI).

Three ping sweeps is normal for something public-facing — anything directly open to the public is going to constantly be scanned. Vulnerability scan results may be an indicator, but the scan itself does not indicate if any vulnerability was found. A CVSS score is a KRI, but a score of 2.1 is so low that it does not need to be remediated right away and is not as important as an active attempted breach occurring through failed authentication attempts.

17.

If a business has a need for high availability of their core servers and they are worried about a disaster such as a fire occurring in their data center, what recovery site would be the **BEST** for them?

Mirror site

Duplicate site

Mobile site

Hot site

Correct answer: Mirror site

A mirror site quite literally mirrors the primary site, at least for the servers and services that require high availability. With a mirror site, both the primary and the secondary site are operational at the same time. A load balancer directs traffic in a distributed manner between them.

A duplicate site could be anything from a hot site to a reciprocal site, but it does require time to bring the site active. A mobile site is defined as moveable, but would not be expected to always be active. A hot site does have all of the IT equipment and operating systems, but it is missing people, data, and possibly programs, which will require a few hours of time to get operational.

18.

What corporate position would the Incident Response Team (IRT) leader hold?

Incident response manager

Information security manager

IT specialists

Investigators

Correct answer: Incident response manager

The incident response manager would be the IRT leader.

The information security manager would be the Incident Management Team (IMT) leader. IT specialists and investigators are subject matter experts needed as team members for both IMT and IRT.

19.

Why would an organization conduct a pretest when testing their operational recovery?

To prepare for a simulation

To test recovery strategies before the simulation

To determine if the plan was effective enough

To determine if the testing is realistic for the environment

Correct answer: To prepare for a simulation

An organization would conduct a pretest before testing their operational recovery to ultimately prepare for a simulation. This pretest prepares everything for the actual test to make sure it can function and do so with accuracy.

The pretest does not actually test recovery strategies — the actual test does that. The test will then determine if the testing meets the needs of the environment and if the plan was effective enough. Testing and improving operational recovery is key to ensuring strong reliability for customers and reduced overall impact on business.

20.

Insurance is a critical part of running a business. Insurance policies have different purposes.

If a business is worried that one of their contractors might make a mistake and cause them financial loss, what type of insurance should the contractor have?

Errors and omissions

Extra expense

Professional and commercial liability

Cybersecurity

Correct answer: Errors and omissions

Errors and omissions insurance is designed specifically for this scenario. If a professional practitioner causes financial loss to a client because of an error or an omission that they made, then this insurance would help to cover that loss.

Extra expense insurance is designed to cover the extra costs that are incurred after damage at the data center. Professional and commercial liability protects a business when a third party claims that the business caused them losses or damage. Cybersecurity helps in the event of something like ransomware, Denial of Service (DoS), or a Distributed DoS (DDoS).

21.

Blaise has determined, with the assistance of his Disaster Recovery (DR) team, that the transactional database for customer sales must be able to process at least 1,000 connections per hour. This is less than the normal processing capability of 1,500 connections per hour. If they are able to accomplish this level of functionality at the hot site, they will be able to ensure the survivability of the business, at least for a while. However, it must return to a normal condition within three weeks.

What is the term for the idea here of 1,000 connections per hour instead of the 1,500 per hour that is the norm?

Service Delivery Objective (SDO)

Maximum Tolerable Outage (MTO)

Recovery Time Objective (RTO)

Allowable Interruption Window (AIW)

Correct answer: Service Delivery Objective (SDO)

The SDO is the level of service that must be supported at the alternate site. Here, it is the reduced number of connections per hour.

The three-week window of time would be the MTO. The RTO is the time to perform the recovery actions to bring customers online at the alternate site. The AIW is the amount of time from nonfunctionality to restoration of critical services.

22.

An organization wants to develop an incident response plan in the event that one of their workstations is infected with malware. Employees know the signs of an infection can include a sluggish computer, locked files, and suspicious programs running.

After identifying this infection, what would management **MOST** likely recommend to prevent it from spreading further?

Immediately disconnect from the network and report to the cybersecurity team

Refrain from acting upon the malware

Document findings yourself

Work around the issue to complete primary tasks at hand

Correct answer: Immediately disconnect from the network and report to the cybersecurity team

While there is controversy around this tactic, the best bet to reduce the spread of the infection is by immediately disconnecting from the network and reporting to the cybersecurity team. Some may say that disconnecting a device from the network could trigger malware to lock up files immediately. If this is going to happen regardless, then you need to ensure more systems aren't affected, as the more systems infected, the greater liability and financial responsibility.

You cannot simply refrain from acting on the malware. From a business perspective, you must do something to prevent the spread, even if it means not being able to fully research the attacker's intentions after. If you are not responsible for investigating such an incident, you should not document the findings yourself while allowing it to spread. You also should not work around the issue and avoid it. Many of these options would be deemed negligent and could void an insurance policy.

23.

An organization has experienced a breach within some of their payment systems and must have an external or third-party audit conducted before the affected systems are brought back to production. What is one step the organization could take to ensure their success in this process?

Conduct an internal audit

Report the incident to an insurance provider

Report the incident to law enforcement

Share this information immediately with information sharing centers (ISACs)

Correct answer: Conduct an internal audit

Prior to any external or third-party audit, an organization would be wise to audit themselves and check their own work before others check it for them. This allows for a simpler audit and a stronger reputation.

Reporting the incident to an insurance provider or law enforcement is important when needed, but it will not ensure success in an external or third-party audit. Sharing information to ISACs is important, but should be done when a vulnerability is remediated. This ensures everyone is educated on the matter, but no threat is posed to your business. Reporting this before the vulnerability is remediated could allow someone to launch an attack, knowing your organization cannot defend against it.

24.

Which of the following **BEST** describes when disaster recovery and business continuity plans should change?

Plans change based on what is impacted, how it is impacted, and how it affects the business overall

Disaster recovery plans should never change

Plans change only when technicians direct that they should

Plans change mainly due to the cost of the asset directly affected

---

Correct answer: Plans change based on what is impacted, how it is impacted, and how it affects the business overall

An organization would have multiple disaster recovery and business continuity plans based on what is impacted, how it is impacted, and how it affects the business overall. For example, a plan for a fast-spreading malware infection would be far different from a plan for a power outage or a motherboard dying. These plans should be created, updated, or replaced with changes to the business, such as the acquisition of a new application.

Disaster recovery plans should undergo periodic changes. These should be driven mainly by the needs of the business, not technicians' preferences or the costs of affected assets.

25.

Dabria is worried that her business is going to experience a disruption caused by an attacker that will disrupt the data center's functionality. They have built a backup site and have successfully tested the Disaster Recovery Plan (DRP). She thinks it would be wise to get an insurance policy that would help to cover the corporate losses due to this disruption.

What would you recommend?

Business interruption

Valuable papers and records

Fidelity coverage

Media reconstruction

Correct answer: Business interruption

Business interruption insurance is to help cover the company's profit loss during Information Technology (IT) disruptions. Cybersecurity could have also applied here, although it is not an option within the provided answers.

Valuable papers and records insurance is related to actual papers, not IT. Fidelity coverage is insurance purchased to cover dishonest or fraudulent employees. Media (software) reconstruction insurance covers damage to the media. There is a bit of overlap in the concepts of each of these different types of insurance, so watch the wording of questions carefully.

26.

Which of the following **BEST** describes the goal of a business impact analysis?

Determine the effect of losing a single component on a business overall

Determine financial losses resulting from replacing an item

Determine financial losses resulting from failing to serve customers

Forecast future losses as a result of current issues

Correct answer: Determine the effect of losing a single component on a business overall

A business impact analysis (BIA) determines the effect of losing a component on an organization as a whole. In losing a component, you can measure how it trickles down and affects the rest of the organization.

In addition to identifying potential financial losses, a BIA also determines how the loss of each asset can result in losses in other critical aspects such as customers or reputation. With this, you can determine how valuable each asset is to the organization; it also helps create a value estimate for insurance purposes.

27.

Danielle has been in discussions with her corporate data service provider. The provider has informed her that, should their long-distance facilities have problems, there are agreements with other providers to switch traffic to their networks. They have also explained that this will happen automatically.

What is the provider describing?

Long-haul network diversity

Last-mile circuit protection

Alternative routing

Diverse routing

Correct answer: Long-haul network diversity

The question describes long-haul network diversity. This is normal practice for carriers today, so that the Wide Area Network (WAN) (such as MPLS (Multiprotocol Label Switching)) or internet access will continue to work, no matter what happens to different wires or facilities.

This is close to diverse routing in nature, but since the question specifies a carrier network, long-haul diversity is the correct answer. Diverse routing is done from the corporation's perspective (the carrier's customer's perspective). Alternative routing is on different media, which is also for the corporation, not the carrier. Last-mile circuit protection is from the carrier to the corporation.

28.

A data center catching on fire would be the result of what type of threat?

Technical

Human-driven

Environmental

External

Correct answer: Technical

Technical threats include fire, heating failures, system and software issues, telecom failure, etc.

Environmental threats include natural disasters. If the fire was a wildfire, then it would be an environmental threat, but it is more likely an internal issue in the building, so technical is the better answer. Human-driven threats arise because of people (disgruntled employees, people taking shortcuts to save time, corporate espionage, embezzlement, etc.). A human may have intentionally set the fire, but there is nothing in the question about that, so one should default to this fire being due to a natural cause. External threats are not one of ISACA's categories.

29.

Within the incident management life cycle phases, when would a forensic analysis occur (when necessary)?

Containment, analysis, tracking, and recovery

Detection, triage, and investigation

Planning and preparation

Postincident assessment

Correct answer: Containment, analysis, tracking, and recovery

According to the ISACA incident management and response document of 2012, forensic analysis occurs within the containment, analysis, tracking, and recovery phase. What is critical to note is that all documents regarding this topic do not show the same thing. This is an ISACA exam, and that is what they have in their incident management and response document. So, if you think it belongs to a different step, you are not necessarily incorrect, but for the exam, consider this set of lifecycle steps as a way to answer questions.

30.

As the information must be accessible to your users when a failover occurs at the Disaster Recovery (DR) site, you are looking into the technologies available to find the best solution to make the data available when it is needed. What parameter is **CRITICAL** to your decision?

Recovery Time Objective (RTO)

Recovery Point Objective (RPO)

Allowable Interruption Window (AIW)

Service Delivery Objective (SDO)

Correct answer: Recovery Time Objective (RTO)

The RTO is the time allowed for the recovery of a business function. This would include the machine, operating system, applications, and data.

The RPO is about the age of the data or the loss of data. The question is looking for "when it is needed." When gets you directly to RTO. Recovery Point Objective (RPO) is still critical, but that is how much you can lose. Allowable Interruption Window (AIW) is very close to the answer here, but we are looking for a technology. The technologies must work within our time window for recovery, RTO. The AIW is the total amount of time the corporation can wait from failure to functionality.

31.

A corporation has determined that it will have to do the work of recovering a critical server within a four-hour window. What is the name of this time period?

Recovery Time Objective (RTO)

Recovery Point Objective (RPO)

Allowable Interruption Window (AIW)

Service Delivery Objective (SDO)

Correct answer: Recovery Time Objective (RTO)

The Recovery Time Objective (RTO) is the amount of time that is allowed for the recovery of a business function.

The recovery must fit within the Allowable Interruption Window (AIW). The AIW is the total time that the corporation can wait between the moment of failure to the restoration of critical services. Once the service is recovered, it needs to be to the Service Delivery Objective (SDO). The SDO is the level of service, e.g., % of transactions/hour.

32.

Incident Response Plans (IRP) must be tailored for a specific business. The basic steps of incident response, though, are consistent. What is the **CORRECT** order of these steps?

Prepare, protect, detect, triage, respond

Prepare, detect, protect, triage, respond

Respond, prepare, detect, triage, protect

Detect, prepare, triage, protect, respond

Correct answer: Prepare, protect, detect, triage, respond

You must first prepare by building teams that create plans to fulfill objectives. Then you protect, and take actions to reduce the chance of specific incidents happening. However, if they do happen, you must then detect them. If you do not know something is happening, then you cannot respond. Response is not the next step; you must triage. You must assess all that is happening to use your limited response resources as effectively as possible. Once you know that information, then you can respond.

33.

During a Business Impact Analysis (BIA), it is essential to identify acceptable downtimes and resource requirements. What else would be considered a **PRIMARY** goal of a BIA?

Criticality prioritization

Management concerns

Legal requirements

Audit capability

Correct Answer: Criticality prioritization

There are three primary goals for a Business Impact Analysis (BIA):

1. *How long can you be without the system (data or other)?*
2. *What resources are required for the system (or other) to function?*
3. *Where in the list of priorities does this fall so that it is recovered within time?*

Management's concerns are essential, but it is not the BIA output. It should be some of the initial information gathered for risk analysis or incident management. The same would be true with legal requirements. It should be information discovered at the beginning of the process, rather than as an output of a BIA. Audit capability is something that is needed from our auditors or for those being audited. It is not typically linked directly to BIA.

34.

As the information security manager, you have been working with the Disaster Recovery Planning (DRP) team. The assessment that you have just completed shows that you could tolerate functioning at a lowered processing level for a little while. The determination is that you could process 5,000 requests per minute as opposed to the usual 8,000.

What is the name of this reduced operations term?

Service Delivery Objective (SDO)

Recovery Time Objective (RTO)

Allowable Interruption Window (AIW)

Maximum Tolerable Outage (MTO)

Correct Answer: Service Delivery Objective (SDO)

The Service Delivery Objective (SDO) is the level of processing that is tolerable for a contained time period.

The time period is the Maximum Tolerable Outage (MTO). The Recovery Time Objective (RTO) and the Allowable Interruption Window (AIW) have to do with the time a service can be offline.

35.

When determining the amount of time that can be taken by the Incident Response Team (IRT) to bring a server back online, the team may find that a contract with one of their customers requires recovery within a certain amount of time. What part of a contract would that be?

Service Level Agreement (SLA)

Master Service Agreement (MSA)

Privacy Level Agreement (PLA)

Data Processing Agreement (DPA)

Correct answer: Service Level Agreement (SLA)

When determining the amount of time that can be taken by the Incident Response Team (IRT) to bring a server back online, the team may find that a contract with one of their customers requires recovery within a certain amount of time. This would be the Service Level Agreement (SLA) part of the contract.

The MSA defines the relationship between the two parties: the customer is responsible for X and then the provider is responsible for Y. The PLA is a notification to the cloud provider that sensitive personal data is in their possession. In Europe, it is referred to as the Data Processing Agreement (DPA), or the Business Associate Agreement (BAA) under HIPAA in the US.

36.

Who is allowed to declare a disaster so that the process to move to the alternate site is initiated after a fire starts in a data center?

It is defined during Disaster Recovery Plan (DRP) creation

The Chief Executive officer (CEO)

A present information security manager

Any member of the Board of Directors (BoD)

Correct answer: It is defined during Disaster Recovery Plan (DRP) creation

Who declares the disaster and under what criteria must be decided upon and documented during the plan creation. It could be the CEO, an information security manager, the Board of Directors (BoD), or someone else. It all depends on the decisions about who can call a disaster and who is on-site or available at the time it needs to be done.

37.

A corporation is working to test their Incident Response Plan (IRP), and they have the recovery team role-playing a prepared scenario without activating the alternate site. What type of test are they doing?

Simulation

Structured walkthrough

Checklist

Parallel

Correct answer: Simulation

In a simulation, the team role-plays through a scenario without activating the alternate site.

A structured walkthrough is a paper-based test to review each step of the written plan. A checklist is a preliminary level test to ensure that the checklist and the plan are current. A parallel test brings the alternate site up while operations continue as they normally are.

38.

If an insurance company is worried about drive failure in one of its critical servers, what would you recommend?

Redundant Array of Inexpensive Disks (RAID) 5

Recovery Time Objective (RTO)

Network Attached Storage (NAS)

Virtual machine

Correct answer: Redundant Array of Inexpensive Disks (RAID) 5

A Redundant Array of Inexpensive Disks (RAID) array is the installation of many drives within a single server. RAID 5 does have the ability to withstand a drive failure within a server. The failed drive is then hot-swappable with a new drive to replace it (the server does not need to be powered down).

Recovery Time Objective (RTO) is the time it would take to bring the server from a failed status to an operational status on a different machine, possibly within a different building. Virtual machines have many uses, but helping a server withstand a drive failure is not one of them; however, they can make it easier to recover the server elsewhere. Network Attached Storage (NAS) is helpful for backing up and recovering data if a drive fails and data loss occurs. Since the question is about a drive failure and RAID 5 is an option, NAS is not the best answer.

39.

Which of the following is **LEAST** likely to be considered by an organization when deciding to have a centralized incident response team?

Services offered and cost

Skill sets

Constant training and educational opportunities

Proper equipment and implementation

Correct answer: Services offered and cost

Services offered and cost would be the least likely consideration by an organization when deciding to have a centralized incident response team, because a centralized team would be in-house, so it could be easily tailored to the needs of the organization. To ultimately save costs, an organization could integrate cost into the salary of a current employee, expand the roles of employees, or create new roles when more employees are needed anyway.

With an in-house team, an organization has to consider the current skill sets of employees and assess where skill sets need to be, while keeping up with constant training and educational opportunities. The organization also has to ensure proper equipment and implementation for maximum benefit.

40.

What word **BEST** describes any event that may cause harm to a corporation and its assets?

- **Threat**
- Vulnerability
- Risk
- Attack

Correct answer: Threat

A threat is any event that can cause harm to a corporation.

A vulnerability is a weakness or flaw (unpatched device, unlocked door, etc.). Risk is the likelihood and its impact combined (there is a 20% chance I will drop my phone today and break the screen). Attack is an action taken by bad actors to exploit a vulnerability and cause the threat to be realized.

41.

What type of test involves planning and brainstorming how an incident might be handled using a tabletop exercise?

Paper test

Preparedness test

Diagram test

Full operational test

Correct answer: Paper test

A paper test involves mapping out a critical incident on paper. These tests are essentially a walkthrough with a diagram included, and they occur early in the testing phase of a response recovery plan.

A preparedness test is a localized test where a simulation occurs and brings the plan to life, allowing the faults or benefits of the plan to become more visible. They can be broken into parts and also evaluated in parts, allowing for a more granular approach to creating a disaster recovery plan.

A full operational test will test the complete plan with a test that falls just short of an actual outage or incident.

Diagram tests are not an actual term associated with the exam.

42.

What is the CMU SEI's five-step incident management process?

Prepare, protect, detect, triage, respond

Identify, prevent, detect, respond, review

Observe, orient, decide, act, repeat

Protect, prepare, detect, triage, respond

Correct answer: Prepare, protect, detect, triage, respond

The five steps of incident management are:

1. ***Prepare** includes designing a network with security controls and creating safety procedures.*
2. ***Protect** consists of implementing protective measures on a network, such as an intrusion prevention system or configuring a firewall.*
3. ***Detect** is using that intrusion detection system to proactively defend the network.*
4. ***Triage** is best defined as ranking incidents and deciding what to manage in order of priority.*
5. ***Respond** is taking action to ensure that the incident doesn't occur again, which can mean taking legal action or patching a system.*

Following these steps in order is essential, as mixing one of them up could lead to poor results and further impact the network.

43.

K.C. is working with her team to understand the current state of incident response within their business. She has a goal of improving their response time and efficiency in closing incidents.

What type of analysis would you recommend for her to get the **MOST** comprehensive and complete view possible of the current state?

- **External assessment**
- Survey of senior management
- Self-assessment
- Internal audit

Correct answer: External assessment

An external assessment should give the most comprehensive view.

A self-assessment or internal audit is probably the easiest option, but they are done against specific criteria and are limited in their view. A survey of senior management is a valuable thing to do, but it will not be the most comprehensive. It is good to obtain their goals and objectives, as well as their current perception of the incident management that does currently exist.

44.

During an incident notification process, which team would be **MOST** likely to respond to an incident?

Physical and information security

Public relations

Cybersecurity

Legal

Correct answer: Physical and information security

Most incidents will involve physical and information security, since any cybersecurity incident will usually involve information and the CIA triad. Additionally, information security personnel define and assign responsibilities, so they must be present.

Public relations would be involved if a breach needed to be announced and the company's reputation was at stake. Cybersecurity teams would play a role in addressing and remediating issues, and ensuring they do not occur again. Legal would only be involved when a criminal or civil matter arises and is necessary to resolve the issue.

45.

Which of the following can be described as a series of storage components connected with fiber cabling that ensures fast data transfer over a LAN connection, and is a central location for data fetching?

SAN (storage attached network)

NAS (network attached storage)

RAID (redundant array of independent disks)

FCOE (fiber cabling over ethernet)

Correct answer: SAN (storage attached network)

A storage attached network (SAN) is a fixed storage facility for anyone to access in the workplace over a network.

A network attached storage (NAS) is typically easier to set up, as it uses regular ethernet cables, and it is cheaper. A SAN, on the other hand, often uses fiber cabling over ethernet (FCOE) for fast data transfers and is generally more expensive. A redundant array of independent disks (RAID) is good for backups, but would back up to a specific user and not an entire workplace.

46.

When a corporation is worried about losing data and they have a very low amount of data that they can tolerate losing, they should utilize:

Synchronous replication

Asynchronous replication

Redundant Array of Independent Disks (RAID) 2

Backup tapes

Correct answer: Synchronous replication

Synchronous replication is when data is written to local and remote storage at the same time.

Asynchronous replication is doing something like backing up data once a day to a backup tape. Synchronous replication would be writing data to drives, not tapes, today. RAID 2 mirrors data, but it is only within a server. So, if they are really worried about losing data, it is best to write it to another location.

47.

What is the primary difference between heuristic analysis and signature analysis?

Heuristic look at traits and code to identify suspicious properties. Signature rely on predefined patterns.

Heuristic rely on predefined patterns. Signature look at traits and code to identify suspicious properties

Signature rely on a predefined baseline and compare it to current behavior. Heuristic rely on traits of a file to determine if it could be malicious.

Heuristic rely on a predefined baseline and compare it to current behavior. Signature rely on traits of a file to determine if it could be malicious.

Correct answer: Heuristic look at traits and code to identify suspicious properties. Signatures rely on predefined patterns.

The primary difference between heuristics and signatures is heuristics look at traits within a file or code, while signatures look at a predefined pattern that makes up a "signature".

Neither one looks at baselines, as that is common with anomaly analysis. However, signature-based analysis requires an associated signature with an attack in order to be identified. Heuristic analysis looks at behavior and traits to determine if software is malicious, regardless of the signature.

48.

Incident management often involves many different roles, along with a joint team effort. Which of the following would an organization be **LEAST** likely to utilize during an incident in which malware was found on a system, but no data was exfiltrated?

Public relations

System techs

Cybersecurity engineers

Internal audit

Correct answer: Public relations

In this scenario, the public relations department isn't needed because there is no public disclosure required.

System techs and cybersecurity engineers need to remove malware and ensure systems are back to normal, which involves sanitizing a drive and migrating data from a backup to a clean system. After this, an internal audit should be conducted to ensure the system meets security requirements. A third-party or external audit will likely have to be conducted prior to the device entering production.

49.

Which of the following is **LEAST** likely to be a resource following a cybersecurity incident?

Sales and marketing

Legal department

Law enforcement

Human resources

Correct answer: Sales and marketing

Sales and marketing would not be a resource after a cybersecurity incident because their expertise is outside of the scope of the issue at hand.

The legal department and law enforcement could be involved if civil or criminal charges are filed, depending on circumstances. Human resources can also be involved if there is an insider threat — an employee may need to be reprimanded or fired as a result of the incident.

50.

Which of the following is **LEAST** likely to be used natively on Linux systems for system hardening?

Procmon

AppArmor

Chmod

Security-enhanced Linux

Correct answer: Procmon

Procmon is least likely to be used natively on Linux systems — it is a Windows program through Microsoft Security Suites.

AppArmor is a command-line application that can control permissions of programs on any Linux system, which is useful for locking down an account. Chmod is a command in Linux to change permissions of a file, folder, or program. Security-enhanced Linux (SELinux) is a command-line application like AppArmor, but allows for more granular permission configuration.

51.

When building a Disaster Recovery Plan (DRP), you have determined that your corporation will likely experience a widespread disaster from an earthquake. The expectation is that the data center equipment will not be able to function anymore. You are looking for a solution that will allow Information Technology (IT) recovery without leaving the region.

What do you recommend?

Mobile site

Hot site

Warm site

Cold site

Correct answer: Mobile site

A mobile site is a specially designed trailer that can be brought in quickly with the equipment you need ready to go inside. They are instrumental in widespread disasters that result in no alternative sites in that region being available.

A hot site is not a suitable answer to the question because we have an earthquake and a desire not to leave the region. If there were an earthquake, the IT equipment would not be usable in the primary or the alternate site. A warm site is not a suitable answer for the same reason as a hot site. If in the same region, what is there would not be usable, and they do not want to leave the region (according to the question). A cold site has a similar problem with location. It does not already have IT equipment, so it would not be broken during an earthquake. But, cold sites are only used in unusual situations, such as tolerating an extended downtime or needing a second backup location. Neither of those situations is mentioned in the question.

52.

When a corporation has determined that they can **ONLY** tolerate a non-functional status for their primary server and database for 2.5 hours, what have they determined?

Acceptable Interruption Window (AIW)

Maximum Tolerable Outage (MTO)

Service Delivery Objective (SDO)

Recovery Point Objective (RPO)

Correct answer: Acceptable Interruption Window (AIW)

The AIW is the time that a server/service can be offline before it is detrimental to a corporation.

The MTO is the time that a business can remain in the alternate processing state, such as having failed over to a hot site. The SDO is the level of service that must be present in the alternate processing mode for it to be suitable for business success. The RPO is the age of the data that can be tolerated once it is recovered to the alternate site.

53.

An unexpected event is called a/an:

- **Incident**
- Disaster
- Problem
- Issue

Correct answer: Incident

By ISACA's definition on page 259, an incident is an unexpected event.

A disaster, as defined on page 277, is recovering an IT-processing facility, operational facility, or IT capabilities. A problem—page 259—is something greater than an incident. They do not actually define what a problem is here. ITIL defines a problem as something that occurs over and over. "Issue" is not an Incident Response (IR) term.

54.

Allen is working at a newspaper company. Even though they have adapted to the paperless environment and have their newspaper online, they still have a printing press and enough demand to keep it running. The company does plan to keep printing newspapers for years to come, even though they have reduced their printing to a single facility. They are worried about a fire that could disrupt printing. They are looking into recovery sites that they could use to keep this service working for their customers. They know that if they stop printing for more than two days they will lose their customers. Allen is tasked with finding the **MOST** cost-effective recovery site possible.

What would you suggest?

Reciprocal agreement

Hot site

Warm site

Mobile site

Correct answer: Reciprocal agreement

Even though reciprocal agreements are not as common as they may have been at one time, it is the best option here. Because they have one printing site and they want to save money, this is the only option that makes sense. They will have to work carefully on the contract and agreement with another newspaper company.

It is much more affordable than having a second printing press at a hot site that is ready to be used when a fire happens. A warm site is not likely to have an expensive printing press there. It can take months to get a new one purchased and installed, and they only have two days. A mobile site is unlikely because printing presses are just too large to fit in something like a trailer.

55.

What are the steps of an incident response plan?

Preparation, Identification, Containment, Eradications, Restoration, Follow-up

Identification, Preparation, Containment, Eradications, Restoration, Follow-up

Identification, Preparation, Containment, Eradications, Follow-up, Restoration

Preparation, Containment, Identification, Eradications, Restoration, Follow-up

---

Correct answer: Preparation, Identification, Containment, Eradications, Restoration, Follow-up

Preparation is commonly added as the first step to incident response. You must build your IRP before an incident happens. After preparation, you need to identify that something may be/is happening. Then, immediately contain the incident so it does not go further. After that, eradicate the attack, virus, attacker, etc. from the systems. Then, restore them to normal. When all is done, have a follow-up/lessons learned/postmortem meeting to uncover what worked and what did not, so that things can be improved in preparation for the next incident.

56.

When a bad actor has successfully installed malware on a critical corporate server and it is now communicating back to the bad actor's server, the attack has progressed to which phase of the kill chain?

Command and control

Installation

Exploitation

Actions on objective

Correct answer: Command and control

When the malware is communicating back to the bad actor's server, the attack is now at command and control.

Installation is when the malware is installed on the corporate server. Exploitation is when the malware takes advantage of a weakness in the target system or network to get to the corporate server. Actions on objective is when the bad actor is able to proceed with their plan because the malware has communicated back after installation.

57.

A recovery site that has partial Information Technology (IT) configurations would be a:

Warm site

Hot site

Cold site

Mobile site

Correct answer: Warm site

A warm site has partial IT equipment and/or IT configurations.

A cold site does not have any IT equipment. A hot site site has the equipment and configurations it needs already in place. A mobile site is a plausible answer, but what defines a mobile site is that it is moveable. Traditionally, the most like configuration within the mobile site or trailer would be at hot site status.

58.

If a security incident has caused the functionality of a critical Information Technology (IT) system to be significantly reduced, what aspect of security has been affected?

Availability

Integrity

Confidentiality

Risk

Correct answer: Availability

Availability means that the system and data must be usable when the end-users need them. If there is a severe reduction in the functionality of a critical system, it can impact the corporation's mission.

Integrity says that the data and system must not be changed or modified inappropriately. Confidentiality means that business secrets must not be protected so that they are not shown to someone not allowed to see that information. Risk is a combination of likelihood and probability.

59.

One of the first tests that should be performed on the Disaster Recovery Plan (DRP) that has the team members talking through the plan and reviewing it on paper **ONLY** is the:

Structured walkthrough

Simulation

Parallel test

Checklist

Correct answer: Structured walkthrough

The structured walkthrough is also known as a tabletop exercise because it occurs in a room while the team members are seated at a table. It is not an exercise that has any actions taken on the network or business processes.

The parallel test brings the alternate site up and operational alongside the functioning business. In other words, the company should not be interrupted.

A simulation is effectively a role-playing game, but the alternate processing capability is not activated. A simple example is a fire drill. You pretend there is a file and physically go through the motions of exiting, but you do not start a fire.

A checklist has the team ensuring that everything that is needed in the plan did in fact end up in the plan.

60.

If a team is performing a forensic analysis, what phase of incident management are they in?

Containment, analysis, tracking, and recovery

Planning and preparation

Detection, triage, and investigation

Post-incident assessment

Correct answer: Containment, analysis, tracking, and recovery

The containment, analysis, tracking, and recovery phase is when a forensic analysis should be performed.

Planning and preparation is when policies are written and tools are acquired. Detection, triage, and investigation is the initial response to an event. In that phase, triage is performed so that the most critical incidents are handled first. Post-incident assessment is when a postmortem is conducted and feedback is given based on lessons learned.

61.

What term is used to describe the redundant cabling with alternative routing in place to **MINIMIZE** the impact of a cable break in the voice communication structure?

Voice recovery

Long-haul network diversity

Recovery Time Objective (RTO)

Redundancy

Correct answer: Voice recovery

Having an alternate cabling structure so that a cut line will not also sever the company's ability to talk to their customers (or anyone else) is called voice recovery. It is a type of redundancy.

Redundancy is not the best option here, since voice recovery matches the description in the question. Long-haul network diversity is redundancy within the service provider's core network. That network could carry data, voice, or video. Recovery Time Objective (RTO) is the time that can be taken to restart a failed service before there is a significant impact on the company.

62.

In what instance would an insurance company be **LEAST** likely to provide coverage after a cybersecurity incident?

Negligence of regulations

Damage to physical systems

Loss of software

Mistakes by employees

Correct answer: Negligence of regulations

An insurance company is least likely to provide coverage after negligence of regulations. Generally, insurance companies provide coverage in agreed-upon circumstances. The amount of coverage and what is covered is based upon making a profit and also being competitive with other companies. Insurance companies would likely make little profit if they covered every instance of negligence.

Insurance companies cover damage to physical systems due to accidents and disasters, loss of software due to unforeseen circumstances, and even honest mistakes by employees. There are a variety of categories within insurance, such as errors and omissions or professional and commercial liability, which are typically covered under insurance.

63.

Suppose a business has been disrupted because of ransomware. The ransomware encrypted 80% of the data needed to function.

What type of plan would be used to recover?

It must be defined within a corporation

Incident Response Plan (IRP)

Emergency management plan

Disaster Recovery Plan (DRP)

Correct answer: It must be defined within a corporation

ISACA uses the following definitions within its 16th edition CISM manual. It is hard to figure out the difference between them. They even state on page 282 that the same words are used to describe a Disaster Recovery Plan (DRP) and a Business Continuity Plan (BCP). Within any given business, it is essential that these terms are defined and clarified. It is critical that they are understandable and consistently used.

Emergency management activities are the events that require prompt attention to recover operational status. Incident Response Plans (IRPs) are used for unplanned interruption of business activities. A Disaster Recovery Plan (DRP) is for preventing, mitigating, and recovering from disruption. A disaster must be declared for this plan to be used.

64.

During an incident response, there are many tasks that need to be completed. Who would write the report on the investigation findings?

Investigator

Incident handler

Information security manger

Legal representative

Correct answer: Investigator

The investigator writes the report on the investigation findings.

The incident handler writes the report on the incident response. This question is not trying to trick you — just watch the wording carefully. The legal representative works to ensure that all actions taken are within legal and regulatory requirements. The information security manager oversees the Incident Management Team (IMT) and possibly the Incident Response Team (IRT). They would not write the investigation findings report, as they were not doing the actual work.

65.

When determining which offsite facility is the best option (e.g., hot site, mobile site, etc.) what is the **MOST** critical thing to know?

- **Recovery Time Objective (RTO)**
- Recovery Point Objective (RPO)
- Business Impact Analysis (BIA)
- Service Delivery Objective (SDO)

Correct answer: Recovery Time Objective (RTO)

The Recovery Time Objective (RTO) is the single biggest influence on the type of alternative site you should choose.

You figure out the RTO by doing a Business Impact Analysis (BIA). RTO is the correct answer, though, because it asks for a "thing to know," not a thing to do. The Recovery Point Objective (RPO) is relevant to data backup types. The Service Delivery Objective (SDO) affects the type and quantity of systems at the alternate site.

66.

When a disaster is declared, that usually indicates that:

Operations need to be moved to an alternate site

It is now time to perform a damage assessment

The Incident Response Plan (IRP) failed

All operations have ceased and the business is likely to fail

---

Correct answer: Operations need to be moved to an alternate site

When an incident occurs, the incident response begins. An incident can escalate to a disaster, but that does not mean that the incident response failed. It could only be able to start the response, but unable to handle everything that must be done due to its scope.

If there are life safety concerns, that must be handled first. Then a damage assessment is performed. If the damage assessment shows that operations will not be recoverable at the primary site within the necessary timeframe for business success (Maximum Tolerable Outage (MTO) and Recovery Time Objectives (RTO)), then a disaster is declared. A disaster declaration means that the Disaster Recovery Plan (DRP) is started. The general purpose of DRPs is to move IT operations to another site or into the cloud. A disaster declaration does not mean the business will fail. If it is not declared and action is not taken to restore systems using the DRP, then the business might fail.

67.

Incident response activities would typically occur in what order?

Detect, triage, contain, restore, and report

Detect, contain, restore, triage, report

Detect, report, contain, triage, restore

Contain, detect, triage, report, restore

Correct answer: Detect, triage, contain, restore, and report

1. *An incident must be **detect**ed for anything else to happen.*
2. *Then **triage** occurs, which will diagnose the incident and prioritize actions to be taken.*
3. *The first action is to **contain** the damage so that it does not get any worse than necessary.*
4. *Once it is contained, it is essential to **restore** the systems to normal.*
5. *The final step is to document and **report** on the incident in total.*

As a side note, containment might occur earlier, depending on the exact incident. For example, if you know your computer is being eaten by a virus (detection), you might contain it by disconnecting it from the network before actual triage occurs. So, the order here is the typical set of steps or, you could say, the theoretical order of the steps.

68.

What could you use as the information security manager to show to the Board of Directors (BoD) and senior management that more work, and probably more money, will be needed to **IMPROVE** incident response capabilities?

Key Goal Indicator (KGI)

Key Risk Indicator (KRI)

Quantitative risk assessment

Incident response objectives

Correct answer: Key Goal Indicator (KGI)

A Key Goal Indicator (KGI) can be used to show management the path that you are on, with the Key Performance Indicators (KPIs) as well, in terms of incident response capabilities. If there is a specific goal and you are not making progress needed to get there, you, the information security manager, can use KGIs and KPIs to show where you are at.

Key Risk Indicators (KRIs) do not show progress toward a goal, rather they have a high probability of predicting risk. The question is about improving response capabilities. A KGI shows where you are heading vs. the Key Risk Indicator (KRI), which shows what could happen. Understanding that risk is also where quantitative risk assessment is used. KGIs and KPIs are relevant towards the incident response objectives. The question asks about the objectives, and, more specifically, how well we are doing toward that goal.

69.

What is the third step in CMU/SEI's incident management process?

Detect

Protect

Respond

Triage

Correct answer: Detect

The steps of CMU/SEI's incident management process are as follows:

1. *Prepare: Prepare for a potential incident by identifying requirements for incident management and developing and implementing plans and processes for managing an incident.*
2. *Protect: Implement changes to the network to reduce the chances of a security incident (e.g., implementing recommendations from a vulnerability scan).*
3. *Detect: Identify unusual behavior via audit logs, data loss prevention, intelligence reports, intrusion detection systems, or SIEM.*
4. *Triage: Categorize incidents into those that should be resolved now, those that can wait, and those that can't be resolved (due to limited resources, etc.)*
5. *Respond: Requires a technical, managerial, or legal response, which can result in analyzing data from an incident, a manager discussing the incident with the cybersecurity team, or prosecution as a result of cybercrime.*

70.

As there are limited resources within a business and certainly within incident management, what is needed to apply those resources **MOST EFFECTIVELY** during an incident?

Effective triage capability

Up-to-date firewalls

Management buy-in

Comprehension of the law

Correct answer: Effective triage capability

The most effective way possible during an incident to minimize the impact is to triage all that is happening first, and to apply the limited resources available.

Up-to-date firewalls are no longer helpful as the incident is occurring. A firewall could have stopped some type of unwanted traffic, but "during an incident" is specified in the question. Management buy-in is essential, but it is now too late to put that in place. The same is true with knowing the law(s) relevant to your business. This needs to be done long before so that any legal requirements are taken into consideration during triage.

71.

Which of the following is **LEAST** likely to result from outsourcing incident response?

- **Enhanced trust**
- Twenty-four hour support
- Risk transfer
- Additional employees to manage

Correct answer: Enhanced trust

Outsourcing incident response will not necessarily enhance trust in security. Typically, organizations outsource to either save money or focus efforts elsewhere. Organizations outsourcing security need to keep in mind that other companies do not have as strong an interest in the overall well-being of the organization as they themselves might.

Many companies for outsourcing security can offer twenty-four hour support, which is a major benefit. There is also some risk transfer involved, as another company is now responsible for the security. Outsourcing is also a great alternative to hiring and managing more employees, as this can be more expensive or tedious.

72.

An organization is assessing the importance of effective and cost-effective incident management. While determining what to focus on most to ensure the success of their business, the organization must also determine what to potentially spend less time and resources on.

Which of the following is **LEAST** likely to deliver maximum value to the organization and its continuity?

Options at the lowest cost

Optimized risk management

Integrated incident management with business goals

Ensuring security controls work alongside the rest of the business continuity and disaster relief plans

---

Correct answer: Options at the lowest cost

While organizations can save money and still have effective defenses, always aiming for options at the lowest cost is not a good idea for the future of an organization. Organizations would likely spend more money in the long run in some areas, and it can open them to greater vulnerabilities and risks if the asset is poorly made.

Optimized risk management involves efficiently managing risks and ensuring a strong return on investment. Integrated business management with business goals is equally important, as stated in The Open Group Architecture Framework (TOGAF). Ensuring any security control works within a business continuity or disaster relief plan is important, as there is no continued protection from an impending threat and business cannot continue without this. Just as it is important to test controls at the main facility, it is equally important to test intrusion prevention systems and intrusion detection systems at the mirror site or hot site.

73.

Malachi has been working with the Security Steering Group (SSG) to build the Incident Management Team (IMT) charter. They have realized that there are some skills missing in the existing team members.

At this time, the budget is tight, so they have decided the **BEST** solution is to have some of the skills covered by:

Virtual/temporary team members

Newly hired dedicated team members

A distributed Incident Response Team (IRT)

A central Incident Response Team (IRT)

Correct answer: Virtual/temporary team members

With a tight budget, it could be best to find team members that they can call on when they need them, as opposed to hiring new team members.

A central or distributed team implies that the employees work with the business. The budget is tight, so hiring new employees with specialized incident response skills does not make sense at this time.

74.

The posttest phase of a Disaster Recovery Plan (DRP) parallel test would:

Have the hot site returned to a hot site status

Include evaluations of the staff as they perform their tasks

Involve a debrief with the Board of Directors (BoD)

Include the submission of test results to relevant regulators

---

Correct answer: Have the hot site returned to hot site status

The posttest phase of a test is the cleanup activities. Return resources to their proper place, disconnect equipment, return personnel to their usual location, delete sensitive data from third-party systems, and so on.

It does not include evaluations, debriefs, or reports. All of that must occur, but it is not during the posttest phase of a test. There are three phases to a test: pretest, test, and posttest.

75.

Which of the following is **NOT** a benefit of a central IRT?

Transfer risk

Reduce cost

Provide control

Increase transparency in all security processes

Correct answer: Transfer risk

With a central IRT, there is no transference of risk. The central IRT has designated in-house employees who manage incident response.

By assigning cybersecurity employees to the central IRT, you can reduce costs by forgoing outsourcing. Additionally, this gives the organization full control over managing security. Having a central IRT also provides transparency in incident management processes for employees and an enhanced opportunity to do the same for customers.

76.

Kamil is working with his team to understand the current state of incident management in his business. As the new information security manager, he does not know where the program stands.

What would be the **EASIEST** for him to do to begin to understand where they are so they can improve?

Self-assessment

External assessment

Survey of senior management

Survey of the line managers

Correct answer: Self-assessment

A self-assessment done by the incident management team will give a good understanding of the current capabilities.

An external assessment would be the most complete and expensive option. To start to understand where they are, a self-assessment is the easiest. Surveys of senior management is great to get an understanding of where they want incident response capabilities to be. It can also help to show their view of the current program. Surveys of the line managers can also show what they are looking for, as well as their views. But again, the question is looking for the easiest option.

77.

If a backup Disaster Recovery (DR) site has a complete infrastructure but is only partially configured in terms of Information Technology (IT), what type of site is it?

Warm site

Hot site

Duplicate site

Cold site

Correct answer: Warm site

A warm site has a complete infrastructure but only partial IT configuration.

A hot site has all of the IT. A duplicate site is functionally similar and can quickly take over for the primary site, which is not possible with only partial IT. A cold site has no IT in place until the site is activated. For the CISM exam: if you disagree with these definitions, you should carefully read page 238.

78.

If a critical resource can only be offline for a very small amount of time, say 24 microseconds, what would the **BEST** choice be?

Server cluster

Redundant Array of Independent Disks (RAID) 5

Synchronous replication

Asynchronous replication

Correct answer: Server cluster

For availability concerns of a resource, it is best to have server clusters. All of the servers are active within the cluster, which should result in no or almost no perceived downtime to the user.

RAID 5 is a way to ensure the data on the drives is not lost, but the question is about the resource being online all of the time. That is a CPU and software topic. Synchronous and asynchronous replications are discussions about data loss as well. The question is about the resource being online.

79.

The steps in an incident response plan are: preparation, identification, containment, eradication, restoration, and lessons learned. In which phase would triage occur?

Identification

Containment

Preparation

Eradication

Correct answer: Identification

In this list of steps, identification would be the correct step to have triage done. Triage is the prioritization and categorization of an incident. That way, if many things are happening, you will know where to direct resources first. So identification includes the direction and triage of events.

Preparation is all of the work before an incident actually happens. Containment is the step in which actions are taken to activate the team, notify stakeholders, obtain evidence, etc. Eradication cannot occur until all of these other steps occur. You must know what has happened and contain it before you can eradicate it.

80.

An organization wants to implement SIEM into their enterprise environment. Of the following, which is a feature that SIEM usually lacks?

Automated response to threats

Remote logging

Information aggregation

Detection and notification of threats

Correct answer: Automated response to threats

Security incident and event management (SIEM) lacks automated responses to threats. This is a feature found in security orchestration, automation and response (SOAR).

However, SIEM can allow for remote logging of all network logs. Additionally, it can aggregate information from multiple sources and allow for simplified threat hunting. SIEM can even be configured to identify and notify of threats. A great open-source SIEM is Security Onion.

81.

Which team would be responsible for relocating services from the alternate site, after a disaster, back to the **PRIMARY** location?

Relocation team

Emergency action team

Incident Response (IR) team

Business Continuity Planning (BCP) team

Correct answer: Relocation team

The relocation team moves operations to the alternate site once a disaster is declared, and then they move operations back.

The emergency action team is the designated first responders. They often deal with scenarios such as fire. The Incident Response (IR) team responds to and repairs damage from something like a rootkit or data breach, but they do not move systems to the alternate site or back. The Business Continuity Planning (BCP) team builds the plans for both DR and BC. Some of the same people may be on the DR or BC team, but the team name is changed for restoration work.

82.

When planning a test for the Disaster Recovery Plan (DRP), Josiah was told that he would be moving and installing the backup telephone equipment the day before the test. What test phase is this work a part of?

Pretest

Test

Posttest

Lessons learned

Correct answer: Pretest

Work done the day before the test is the pretest. These actions would not be done during an actual event in this manner, though.

The test phase is during, whereas Josiah is on the day before the test. The posttest phase is after the test and again, he is doing this work a day before. Lessons learned would also be after something has been tested or even an actual incident has occurred.

83.

The Carnegie Mellon University Software Engineering Institute (CMU SEI) defines three types of incident response activities. They are:

Technical, Management, and Legal

Technical, Management, and Human Resources

Management, Legal, and Human Resources

Technical, Legal, and Human Resources

Correct answer: Technical, Management, and Legal

CMU SEI defines the three types of incident response as:

- *Technical (analyzing logs, collecting data, etc.)*
- *Management (notification, escalation, etc.)*
- *Legal (investigation, liability, prosecution, etc.)*

84.

As the information security manager, you know that the Recovery Time Objective (RTO) for critical systems must be determined and this is done during the:

Business Impact Assessment (BIA)

Risk assessment

Incident response

Disaster response

Correct answer: Business Impact Assessment (BIA)

The BIA is part of the process of developing a Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP). It is a combination of a risk assessment and the determination of timeframes, such as RTO.

Determining the timeframe for recovering a system must be done before an incident or disaster response occurs.

85.

Incident management should be aligned with:

Strategic goals and objectives

Laws and regulations

Audit and compliance assessment goals

Known incident management techniques

Correct answer: Strategic goals and objectives

Everything we do in security needs to be aligned with the organization's goals and objectives. This includes incident management.

A company's senior management should ensure that laws and regulations are acknowledged in their goals and objectives, but it is the strategic goals and objectives that incident management should be aligned with. Audit and compliance goals are good to have. The enterprise goals and objectives should also drive those, but there is no direct link from compliance goals to incident management. Known incident management techniques are good to utilize as incident response plans are built, but that is not what incident management aligns with.

86.

Which of the following is **NOT** an incident response responsibility?

Budgeting

Response plans

Confirming safety measures are in place

Call lists or notifying people

Correct answer: Budgeting

Because budgeting is not a way to directly manage a current threat, it is not an incident response responsibility.

Response plans detailing what exactly to do in a given situation could prove useful, especially in stressful situations. Knowing what to do ahead of time allows for more focus during the incident as well. Confirming safety measures are in place is important, as it prevents others from being harmed or otherwise affected by the incident. Additionally, all incident responders should be on a call list or notify others of an incident to ensure a quick and informed response.

87.

Your corporation has been able to determine that it cannot tolerate any data loss due to a disaster. If a transaction has been committed to the database, it must be recoverable if ransomware has hit the business.

They have now defined the:

Recovery Point Objective (RPO)

Recovery Time Objective (RTO)

Maximum Tolerable Outage (MTO)

Allowable Interruption Window (AIW)

Correct answer: Recovery Point Objective (RPO)

The Recovery Point Objective (RPO) is effectively the age of the data that a corporation needs to restore in the event of a disaster. In other words, it is the amount of data they can tolerate losing.

The Recovery Time Objective (RTO) is the length of time for the interruption. The Maximum Tolerable Outage (MTO) is the time allowed in the alternate mode. The Allowable Interruption Window (AIW) is the total time the corporation can wait for services to be restored. All of the incorrect options are a time frame regarding functionality, not the data itself.

88.

Which of the following is **LEAST** likely to be defined as a security incident?

A monitor cracking during installation

Misusing resources

An employee rerouting information to an unknown DNS server

A secretary sharing sensitive information with a caller claiming to be the CIO

Correct answer: A monitor cracking during installation

A monitor cracking during installation would probably not be deemed a security incident as long as nobody is hurt. We also don't know the reason behind the monitor cracking, so an employee may not be responsible — it could have been broken and gone unnoticed until received. This is something that would require more investigation.

Misusing resources can be a violation of a workplace acceptable use policy (AUP). An employee rerouting information to an unknown DNS server is a sign of data exfiltration. A secretary sharing sensitive information with a caller claiming to be the CIO is an example of phishing, specifically vishing. In some of these instances, human resources would have to intervene and talk with employees, and cybersecurity training would also be required.

89.

You are about to perform a test on the Disaster Recovery Plan (DRP) that will bring the hot site to operational status. The running processes within the business will not be interrupted.

What type of test are you doing?

Parallel

Full interruption

Simulation

Structured walkthrough

Correct answer: Parallel

A parallel test has the recovery site brought to an operational state. Still, it is effectively running in parallel to the business because the business is not interrupted in any way.

A full interruption shuts down the primary site and causes a failover to the alternate location. A simulation is a role-playing activity, so nothing is brought operational. A structured walkthrough is a paper-based test to determine the completeness of the DRP document.

90.

An organization needs to develop a geographically separated set of sites that replicate their primary location. This will allow for similar operations everywhere, while also evenly distributing the work between sites.

What does this **BEST** describe?

Mirror site

Mobile sites

Disaster recovery as a service

Hot site

Correct answer: Mirror site

A mirror site is an exact replica of the primary location, and therefore allows for similar operations and redundancy. Additionally, a load balancer can ensure these sites get even workloads in terms of internet traffic.

A mobile site is a site, usually not on the same scale as the original site, which can travel when needed. Disaster recovery as a service (DRaaS) is simply disaster recovery and business continuity in the cloud. A hot site is very similar to the original site, but the CPUs may not be the same — this will ultimately affect workloads and will not allow for similar operations.

91.

A business has just experienced a severe incident. During that incident, their most critical server was offline for an extended period of time. The Incident Response Team (IRT) attempted to restore the system quickly but failed to get it operational within the expected time window.

What is the **LIKELY** reason this could have happened?

A Business Impact Assessment (BIA) was not conducted.

They failed to pay attention to legal restoration requirements.

The auditors did not do a full review of the plan before use.

Senior management was not present during the plan review.

Correct Answer: A Business Impact Assessment (BIA) was not conducted.

A Business Impact Assessment (BIA) is often a missed step in the creation of an Incident Response Plan (IRP). It is essential to understand the impact of a system's loss on the business in order to build appropriate plans. There is little information to work off of in this question, but it is a reasonable guess based on common problems.

There can be requirements for some businesses to have to be operational within a specific time period, but that is unusual. There is no info in the question that this business is a type that would fall under such laws (e.g., national infrastructure). It is not standard practice to have auditors review the plan as a part of incident response planning. During an audit, it could be done depending on the scope, but there is no indication in the question that that is the case. It would not be usual practice to have senior management present during a plan review. They should be advised of the reviews, depending on the situations addressed.

92.

The information security manager in charge of the Incident Management Team (IMT) left the business abruptly. What challenge will the team **MOST LIKELY** face from here on?

Incident Management Team (IMT) member turnover

Mismatch to organizational goals and structure

Overly complex and broad plans

Lack of communication process

Correct answer: Incident Management Team (IMT) member turnover

What is likely, given the lack of info in the question, is that there will be a high member turnover following the abrupt departure from the business. This is not a guarantee for any specific business. It is just a simple scenario to get us to look at and talk about this challenge. Remember the exam is about the rules, not the exceptions to the rules. With the lack of info in the question, it is the best answer because it is specifically connected. The manager is a member of the team. Otherwise, all of the other options could be the source of challenges within businesses today.

93.

Which team would be responsible for coordinating the activities of **ALL** other recovery teams during Incident Response (IR)?

Emergency management team

Emergency action team

Relocation team

Damage assessment team

Correct answer: Emergency management team

This is the emergency management team's job, along with handling key decision-making.

The emergency action team is the first responders to incidents such as fire. The relocation team is responsible for coordinating the process of moving to the alternate site and back again. The damage assessment team is well-named: it assesses the damage. This assessment is what allows management to declare if there is a disaster or not. When a disaster is declared, the work to recover it to another site begins.

94.

If an Incident Management Team (IMT) is in the process of determining the amount of time that is required to recover a specific server, what are they doing?

- **Business Impact Analysis (BIA)**
- Quantitative risk analysis
- Qualitative risk analysis
- A tabletop test

Correct answer: Business Impact Analysis (BIA)

A Business Impact Analysis (BIA) is part of a risk assessment (both quantitative and qualitative). A BIA is designed to identify the most critical resources to the organization and the impact of its loss. A BIA goes on past risk assessment to determine the required recovery time (Recovery Time Objective (RTO)), which is essential for incident management.

A tabletop test is a test designed to logically talk through a planned course of action to see if it is reasonable.

95.

While working through the protect phase of the incident response lifecycle, a known issue is discovered on a server. The server is subsequently fixed.

The issue is called a:

- **Vulnerability**
- Incident
- Threat
- Patch

Correct answer: Vulnerability

A vulnerability is a weakness in a system (or other places).

The vulnerability could be exploited and result in a compromise. The compromise would be an incident. The patch is the standard fix for weaknesses within the code of a server, its Operations System (OS), or applications. The threat is the damage that this incident could cause.

96.

Which of the following is a network of connected devices that has the single purpose of holding and managing a corporation's data?

Storage Area Network (SAN)

Network Attached Storage (NAS)

Direct Attached Storage (DAS)

Redundant Array of Inexpensive Disks (RAID)

Correct answer: Storage Area Network (SAN)

A Storage Area Network (SAN) is a network of interconnected storage devices designed specifically to hold and manage a corporation's data. SANs provide high-performance, scalable storage solutions, making them ideal for large enterprises with significant data storage needs.

Network Attached Storage (NAS) is a single device or set of devices that connect directly to a network, providing shared access to data at the file level, but it does not involve a specialized network like a SAN.

Direct Attached Storage (DAS) refers to storage directly attached to a computer or server, lacking the network connectivity characteristic of a SAN.

Redundant Array of Inexpensive Disks (RAID) is a data storage technology that combines multiple disks into a single system to improve performance and redundancy, usually implemented within a server or a storage device, not across a network of devices.

97.

Creating an incident response plan ensures everyone in the organization understands their role when the time comes. What is the **MOST** proactive way to ensure this goes to plan when an incident occurs?

Have senior management review and sign off on it

Build rapport with co-workers in the same department

Ensure all departments have strong relationships

Make the plan simple and effortless for all

Correct answer: Have senior management review and sign off on it

By having management review and sign off on an incident response plan, it is likely to be enforced and followed by everyone in the workplace because senior management has overall control in the workplace and can make rules as needed.

While building rapport with co-workers, ensuring all departments have strong relationships, and creating a simple plan may help, it isn't anywhere close to a guarantee that the incident response plan will be followed. Management approval is the closest one can get to ensuring an incident response plan goes into effect correctly.

98.

Decisions during a disaster response need to be made by trained and knowledgeable people. This would be:

Managed at the command and control center

Handled by internal communication

Done by the legal team due to fear of mistakes

Only done by the senior management of the business

Correct answer: Managed at the command and control center

The person or team of people that can make key decisions during a disaster response should be found at the command and control center or emergency management center. Communication about the decisions may be done through an internal communication system, but the decisions are made at command and control.

Having the legal team make the decisions due to fear of mistakes does not make much sense. It is possible that mistakes will be made and that advice from lawyers is needed, but to counteract the fear of making mistakes, the better action is to train and practice for incidents before they happen. Senior management may also be on hand for advice. It is possible that some of the biggest decisions will be made by senior management, but they should be at the command and control center to work with and be advised by the team.

99.

If an intruder is creating malware to compromise a corporate server, they are at what stage of the kill chain?

Weaponization

Reconnaissance

Installation

Exploitation

Correct answer: Weaponization

Creating the malware would be weaponization.

Reconnaissance is when research is being done. Installation is getting the malware into the target server. Exploitation is when the weakness in the network/server/human is taken advantage of to get the malware to the target system.