CISA Domain 4 Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. What does applying a retention date on a file ensure?

A. Data cannot be read until the date is set.

B. Data will not be deleted before that date.

C. Backup copies are not retained after that date.

D. Datasets with the same name are differentiated.

2. What is the greatest concern when incidents are assigned incorrect priorities and fail to meet the business service level agreement?

A. The support model was not approved by senior management

B. The incident resolution time specified in the SLA is not realistic

C. There are inadequate resources to support the applications

D. The support model was not properly developed and implemented

3. What is the primary objective of testing a business continuity plan?

A. Familiarize employees with the business continuity plan.

B. Ensure that all residual risk is addressed.

C. Exercise all possible disaster scenarios.

D. Identify limitations of the business continuity plan.

4. What is the MAIN purpose for periodically testing offsite disaster recovery facilities?

A. Protect the integrity of the data in the database

B. Eliminate the need to develop detailed contingency plans

C. Ensure the continued compatibility of the contingency facilities

D. Ensure that program and system documentation remains current

5. What should an organization do if their business continuity plan is outdated?

A. Communicate it to all users immediately

B. Start developing a new plan

C. Regularly update the existing plan

D. Store it in an alternate location

6. What is the best recommendation when notification systems could be impacted during a business continuity simulation?

A. Train the salvage team on the notification system

B. Ensure recovery of the backup systems

C. Build redundancies into the notification system

D. Store the notification systems in a vault

7. What is the greatest concern an IS auditor should have during a review of a disaster recovery hot site?

A. Physical security controls at the hot site are less robust than at the main site.

B. Disk space utilization data are not kept current.

C. Servers at the hot site do not have the same specifications as at the main site.

D. System administrators use shared accounts which never expire at the hot site.

8. What factor is critical in selecting a third-party vendor for backup storage services?

A. Geographic proximity to the organization

B. Proven track record with similar businesses

C. Compliance with relevant privacy regulations

D. Capacity for data volume managed

9. Understanding which of the following is critical for maintaining compliance with internal service levels?

A. Service delivery objectives

B. Contractual obligations

C. Auditing vendor agreements

D. Capacity planning

10. What is a detective control that does not ensure the integrity of data in a database?

A. Authentication controls

B. Commitment and rollback controls

C. Read/write access log controls

D. Data normalization controls

Answers

1. B
2. D
3. D
4. C
5. C
6. C
7. B
8. C
9. A
10. C

Explanations

1. What does applying a retention date on a file ensure?

A. Data cannot be read until the date is set.

B. Data will not be deleted before that date.

C. Backup copies are not retained after that date.

D. Datasets with the same name are differentiated.

Applying a retention date on a file is a critical practice in data management and governance. By setting a retention date, the organization establishes a timeframe during which the data must be preserved. This ensures that the data will not be deleted or disposed of before the specified date has passed, which is important for compliance with legal, regulatory, and organizational policies. Such a mechanism helps in maintaining data integrity and availability for audits or legal proceedings, as it guarantees that relevant data can be accessed for the duration of its retention period. It aids organizations in adhering to retention schedules that dictate how long different types of data should be kept before they can be purged or archived. Other options do not accurately reflect the function of a retention date—data can still be read before this date, backup retention policies are separate considerations, and while naming conventions might assist with data organization, they do not relate to retention.

2. What is the greatest concern when incidents are assigned incorrect priorities and fail to meet the business service level agreement?

A. The support model was not approved by senior management

B. The incident resolution time specified in the SLA is not realistic

C. There are inadequate resources to support the applications

D. The support model was not properly developed and implemented

Assigning incorrect priorities to incidents that fail to meet the business service level agreement (SLA) is primarily a concern regarding the integrity and effectiveness of the support model. A support model outlines how incidents should be categorized, prioritized, and managed within an organization. If the model is not properly developed and implemented, it can lead to misclassification of incidents, incorrect prioritization, and ultimately, delayed resolution times. This misalignment can significantly impact the organization's ability to meet its SLAs, as the support staff may not address critical incidents quickly enough, leading to dissatisfaction from business stakeholders. A well-structured support model incorporates clear guidelines and criteria for prioritizing incidents based on their impact and urgency. If this framework is flawed or inadequately utilized, it results in a cascading effect where resources are misallocated, and high-impact incidents may receive lower priority, adversely affecting business operations and customer satisfaction. Thus, addressing the foundational aspects of the support model is crucial to ensuring that priority assignments reflect the true needs of the business, fulfilling SLAs appropriately. The other options may have some relevance to incident management, but they do not directly alleviate the core issue of misalignment in incident prioritization and SLA fulfillment as comprehensively as the development and implementation of the support model

3. What is the primary objective of testing a business continuity plan?

A. Familiarize employees with the business continuity plan.

B. Ensure that all residual risk is addressed.

C. Exercise all possible disaster scenarios.

D. Identify limitations of the business continuity plan.

The primary objective of testing a business continuity plan is to identify limitations of the plan. Testing is critical as it reveals how well the plan works in practice, highlighting areas that may not function as intended or identifying gaps that could hinder recovery efforts during an actual incident. By actively engaging with the business continuity plan, organizations can discover weaknesses, assess the effectiveness of response strategies, and make necessary adjustments to enhance resilience. Familiarization of employees with the business continuity plan is important, but it is secondary to the goal of assessing the plan's limitations. While exercising disaster scenarios can provide valuable insights into potential responses, the overarching aim is to pinpoint areas where the plan may fall short. Additionally, addressing all residual risk is an ongoing process rather than the primary purpose of testing; the focus during testing is on understanding how well the established procedures perform under stress.

4. What is the MAIN purpose for periodically testing offsite disaster recovery facilities?

A. Protect the integrity of the data in the database

B. Eliminate the need to develop detailed contingency plans

C. Ensure the continued compatibility of the contingency facilities

D. Ensure that program and system documentation remains current

The primary purpose of periodically testing offsite disaster recovery facilities is to ensure the continued compatibility of the contingency facilities. Regular testing helps verify that the infrastructure, equipment, and technology at the offsite location work effectively with the organization's systems and applications. This is crucial because systems and software can change over time; therefore, it's vital to confirm that the offsite facilities can operate seamlessly if the need arises. When these facilities are tested, any discrepancies or incompatibilities can be identified, allowing for timely updates or modifications to ensure readiness in the event of a disaster. This practice not only helps to affirm the practicality of the recovery plan but also enhances confidence among stakeholders regarding the organization's ability to handle crises effectively. The focus on compatibility highlights the importance of maintaining functional and current disaster recovery sites that can be enacted without significant delays, safeguarding operations and minimizing potential downtime during actual emergencies.

5. What should an organization do if their business continuity plan is outdated?

A. Communicate it to all users immediately

B. Start developing a new plan

C. Regularly update the existing plan

D. Store it in an alternate location

The best course of action when a business continuity plan is outdated is to regularly update the existing plan. Regular updates are crucial for ensuring that the plan reflects current business processes, technology, potential threats, and regulatory requirements. An outdated plan may not address recent changes in the organization, such as shifts in operational procedures, changes in personnel, or new risks that have surfaced. By prioritizing regular updates, organizations can maintain their readiness and resilience in the face of disruptions. This proactive approach helps ensure that the strategies in the business continuity plan remain relevant and effective, enabling the organization to recover quickly from incidents or crises. Other options, while they may seem relevant, do not address the issue as effectively. Notifying all users immediately about an outdated plan does not provide a solution; instead, it may cause confusion if the plan is not current. Developing a new plan altogether may be unnecessary if the existing plan can be updated effectively. Storing an outdated plan in an alternate location does not improve its functionality or relevance. Regular updates are essential for maintaining the integrity and efficiency of the business continuity plan.

6. What is the best recommendation when notification systems could be impacted during a business continuity simulation?

A. Train the salvage team on the notification system

B. Ensure recovery of the backup systems

C. Build redundancies into the notification system

D. Store the notification systems in a vault

Building redundancies into the notification system is the best recommendation when considering potential impacts during a business continuity simulation. Redundancies enhance the reliability of communication methods, ensuring that notifications can still be sent and received even if primary systems fail. This proactive measure minimizes the risk of communication breakdowns, which can be critical during an emergency or disaster recovery scenario. Establishing redundancies might involve having alternative communication channels, such as secondary messaging systems or backup networks, which can take over if the primary notification system is compromised. This not only helps maintain essential communication during a crisis but also supports a quicker response time, enhancing overall business continuity efforts. While training the salvage team on the notification system is beneficial, it does not directly address the potential for system failure. Ensuring the recovery of backup systems is important, yet it does not specifically mitigate the risk to the notification systems during the simulation itself. Storing notification systems in a vault may protect them physically but does not ensure operational readiness or accessibility during an event. Redundancy, however, plays a crucial role in maintaining communication integrity and effectiveness in real-time scenarios.

7. What is the greatest concern an IS auditor should have during a review of a disaster recovery hot site?

A. Physical security controls at the hot site are less robust than at the main site.

B. Disk space utilization data are not kept current.

C. Servers at the hot site do not have the same specifications as at the main site.

D. System administrators use shared accounts which never expire at the hot site.

The greatest concern during a review of a disaster recovery hot site is related to how well the disk space utilization data is kept current. Accurate and up-to-date disk space utilization data is crucial for maintaining proper functionality and ensuring that the systems can effectively handle the recovery process when needed. If this data is not current, it can lead to several issues such as inefficient resource allocation, difficulty in managing workloads, or even critical system failures during an actual disaster recovery scenario. Maintaining current disk space utilization data ensures that there is enough capacity to restore operations smoothly without interruptions. It also aids in the planning for additional resources if needed, allowing for timely decisions regarding the acquisition of further storage or adjustments to the disaster recovery plan. In the context of disaster recovery, timely and accurate data is essential for the success of recovery efforts. Therefore, an IS auditor should prioritize this aspect as it directly impacts the effectiveness of the disaster recovery site. The other options, while they might pose concerns, do not directly impact the immediate operational readiness and resource management as significantly as outdated disk space utilization data does.

8. What factor is critical in selecting a third-party vendor for backup storage services?

A. Geographic proximity to the organization

B. Proven track record with similar businesses

C. Compliance with relevant privacy regulations

D. Capacity for data volume managed

Selecting a third-party vendor for backup storage services requires careful consideration of various factors, and compliance with relevant privacy regulations is critical for several reasons. Firstly, vendors that adhere to privacy regulations ensure that data is managed and protected according to legal standards, which is essential for safeguarding sensitive information. Compliance indicates that the vendor has implemented necessary security measures to protect data from unauthorized access and breaches, thus reducing the organization's risk profile. This is particularly important in industries that handle personal or sensitive information, where non-compliance can lead to severe legal implications and financial penalties. Furthermore, vendors that comply with privacy regulations typically have established protocols for data handling, storage, and destruction, which fosters trust and confidence in their services. Organizations are increasingly held accountable for data protection, making it imperative to partner with vendors who prioritize compliance to align with internal governance and risk management frameworks.

9. Understanding which of the following is critical for maintaining compliance with internal service levels?

A. Service delivery objectives

B. Contractual obligations

C. Auditing vendor agreements

D. Capacity planning

Maintaining compliance with internal service levels hinges significantly on understanding service delivery objectives. Service delivery objectives define the expected level of service provided to users, outlining key performance indicators (KPIs) such as response times, availability, resolution times, and overall service quality. By comprehensively understanding these objectives, an organization can effectively measure its performance against the established benchmarks, ensuring that service levels are not only met but also consistently maintained. This focus on service delivery objectives creates a framework within which all operational activities can align. It is vital for continuous monitoring and improvement, as any deviations from these objectives can be promptly identified and addressed. This awareness of service delivery goals empowers teams to prioritize their efforts, enhance customer satisfaction, and drive accountability within the service management processes. While the other options provide important aspects of compliance—such as contractual obligations ensuring legal adherence, auditing vendor agreements to verify adherence to standards, and capacity planning for optimizing resources—they do not specifically address the ongoing management and evaluation of service delivery. In contrast, service delivery objectives are essential for guiding and assessing the organization's adherence to its defined service levels.

10. What is a detective control that does not ensure the integrity of data in a database?

A. Authentication controls

B. Commitment and rollback controls

C. Read/write access log controls

D. Data normalization controls

The correct answer is that read/write access log controls are a type of detective control but do not ensure the integrity of data in a database. Detective controls are designed to identify security breaches or compliance failures after they occur, providing an audit trail that can help in detecting unauthorized access or changes to data. While access logs can show who accessed or modified data and when, they do not actively modify or protect the data itself. In contrast, other controls mentioned play different roles in maintaining data integrity. Authentication controls are focused on verifying the identity of users before granting access, thereby preventing unauthorized actions that could compromise data integrity. Commitment and rollback controls are mechanisms used in database transactions to ensure that either all parts of a transaction are completed successfully or none at all, which is crucial for maintaining data integrity. Data normalization involves organizing data efficiently in a database to reduce redundancy and dependency, contributing to consistent and reliable data integrity. Thus, while read/write access log controls provide valuable insights and a means to detect issues, they do not implement measures that protect or ensure the integrity of the data itself.