ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: ISC2

Code: CISSP

Exam: Certified Information Systems Security Professional

https://www.examsnest.com/exam/cissp/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 42.0

Topic 1, Exam Pool A

Question: 1

All of the following items should be included in a Business Impact Analysis (BIA) questionnaire EXCEPT questions that

A. determine the risk of a business interruption occurring

B. determine the technological dependence of the business processes

C. Identify the operational impacts of a business interruption

D. Identify the financial impacts of a business interruption

Answer: A

Explanation:

A Business Impact Analysis (BIA) is a process that identifies and evaluates the potential effects of natural and man-made disasters on business operations. The BIA questionnaire is a tool that collects information from business process owners and stakeholders about the criticality, dependencies, recovery objectives, and resources of their processes. The BIA questionnaire should include questions that:

Identify the operational impacts of a business interruption, such as loss of revenue, customer satisfaction, reputation, legal obligations, etc.

Identify the financial impacts of a business interruption, such as direct and indirect costs, fines, penalties, etc.

Determine the technological dependence of the business processes, such as hardware, software, network, data, etc.

Establish the recovery time objectives (RTO) and recovery point objectives (RPO) for each business process, which indicate the maximum acceptable downtime and data loss, respectively

The BIA questionnaire should not include questions that determine the risk of a business interruption occurring, as this is part of the risk assessment process, which is a separate activity from the BIA. The risk assessment process identifies and analyzes the threats and vulnerabilities that could cause a business interruption, and estimates the likelihood and impact of such events. The risk assessment process also evaluates the existing controls and mitigation strategies, and recommends additional measures to reduce the risk to an acceptable level.

Question: 2

Which of the following actions will reduce risk to a laptop before traveling to a high risk area?

A. Examine the device for physical tampering

B. Implement more stringent baseline configurations

C. Purge or re-image the hard disk drive

D. Change access codes

Answer: C

Explanation:

Purging or re-imaging the hard disk drive of a laptop before traveling to a high risk area will reduce the risk of data compromise or theft in case the laptop is lost, stolen, or seized by unauthorized parties. Purging or re-imaging the hard disk drive will erase all the data and applications on the laptop, leaving only the operating system and the essential software. This will minimize the exposure of sensitive or confidential information that could be accessed by malicious actors. Purging or re-imaging the hard disk drive should be done using secure methods that prevent data recovery, such as overwriting, degaussing, or physical destruction.

The other options will not reduce the risk to the laptop as effectively as purging or re-imaging the hard disk drive. Examining the device for physical tampering will only detect if the laptop has been compromised after the fact, but will not prevent it from happening. Implementing more stringent baseline configurations will improve the security settings and policies of the laptop, but will not protect the data if the laptop is bypassed or breached. Changing access codes will make it harder for unauthorized users to log in to the laptop, but will not prevent them from accessing the data if they use other methods, such as booting from a removable media or removing the hard disk drive.

Question: 3

Which of the following represents the GREATEST risk to data confidentiality?

A. Network redundancies are not implemented

B. Security awareness training is not completed

C. Backup tapes are generated unencrypted

D. Users have administrative privileges

Answer: C

Explanation:

Generating backup tapes unencrypted represents the greatest risk to data confidentiality, as it exposes the data to unauthorized access or disclosure if the tapes are lost, stolen, or intercepted. Backup tapes are often stored off-site or transported to remote locations, which increases the chances of them falling into the wrong hands. If the backup tapes are unencrypted, anyone who obtains them can read the data without any difficulty. Therefore, backup tapes should always be encrypted using strong algorithms and keys, and the keys should be protected and managed separately from the tapes.

The other options do not pose as much risk to data confidentiality as generating backup tapes unencrypted. Network redundancies are not implemented will affect the availability and reliability of the network, but not necessarily the confidentiality of the data. Security awareness training is not completed will increase the likelihood of human errors or negligence that could compromise the data, but not as directly as generating backup tapes unencrypted. Users have administrative privileges will grant users more access and control over the system and the data, but not as widely as generating backup tapes unencrypted.

Question: 4

What is the MOST important consideration from a data security perspective when an organization plans to relocate?

A. Ensure the fire prevention and detection systems are sufficient to protect personnel

B. Review the architectural plans to determine how many emergency exits are present

C. Conduct a gap analysis of a new facilities against existing security requirements

D. Revise the Disaster Recovery and Business Continuity (DR/BC) plan

Answer: C

Explanation:

When an organization plans to relocate, the most important consideration from a data security perspective is to conduct a gap analysis of the new facilities against the existing security requirements. A gap analysis is a process that identifies and evaluates the differences between the current state and the desired state of a system or a process. In this case, the gap analysis would compare the security controls and measures implemented in the old and new locations, and identify any gaps or weaknesses that need to be addressed. The gap analysis would also help to determine the costs and resources needed to implement the necessary security improvements in the new facilities.

The other options are not as important as conducting a gap analysis, as they do not directly address the data security risks associated with relocation. Ensuring the fire prevention and detection systems are sufficient to protect personnel is a safety issue, not a data security issue. Reviewing the architectural plans to determine how many emergency exits are present is also a safety issue, not a data security issue. Revising the Disaster Recovery and Business Continuity (DR/BC) plan is a good practice, but it is not a preventive measure, rather a reactive one. A DR/BC plan is a document that outlines how an organization will recover from a disaster and resume its normal operations. A DR/BC plan should be updated regularly, not only when relocating.

Question: 5

A company whose Information Technology (IT) services are being delivered from a Tier 4 data center, is preparing a companywide Business Continuity Planning (BCP). Which of the following failures should the IT manager be concerned with?

A. Application

B. Storage

C. Power

D. Network

Answer: A

Explanation:

A company whose IT services are being delivered from a Tier 4 data center should be most concerned with application failures when preparing a companywide BCP. A BCP is a document that describes how an organization will continue its critical business functions in the event of a disruption or disaster. A BCP should include a risk assessment, a business impact analysis, a recovery strategy, and a testing and maintenance plan.

A Tier 4 data center is the highest level of data center classification, according to the Uptime Institute. A Tier 4 data center has the highest level of availability, reliability, and fault tolerance, as it has multiple and independent paths for power and cooling, and redundant and backup components for all systems. A Tier 4 data center has an uptime rating of 99.995%, which means it can only experience 0.4 hours of downtime per year. Therefore, the likelihood of a power, storage, or network failure in a Tier 4 data center is very low, and the impact of such a failure would be minimal, as the data center can quickly switch to alternative sources or routes.

However, a Tier 4 data center cannot prevent or mitigate application failures, which are caused by software bugs, configuration errors, or malicious attacks. Application failures can affect the functionality, performance, or security of the IT services, and cause data loss, corruption, or breach. Therefore, the IT manager should be most concerned with application failures when preparing a BCP, and ensure that the applications are properly designed, tested, updated, and monitored.

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: ISC2

Code: CISSP

Exam: Certified Information Systems Security Professional

https://www.examsnest.com/exam/cissp/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation