Module 8 Assessment (Security Operations & Security Administration and Planning 3rd)

Due Nov 12 at 11:59pm **Points** 20 **Questions** 20 **Available** Oct 30 at 1am - Nov 13 at 11:59pm
Time Limit 45 Minutes **Allowed Attempts** 2

Instructions

You have two attempts to take this assessment with the highest score being retained. The assessment has a time limit of 45 minutes.

Suggestion: take the assessment in the beginning of the module and then after the reading and assignments are done. You can then use the results of both to gauge your learning and retention.

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	17 minutes	16 out of 20

Answers will be shown after your last attempt

Score for this attempt: **16** out of 20
Submitted Nov 6 at 11:31am
This attempt took 17 minutes.

Question 1

1 / 1 pts

Which of the following statements accurately describes a certification process in the context of certification and accreditations?

● Several steps to evaluate, describe, and test a system and all of the controls that are in place to mitigate risks to the system

○ A formal declaration that the system is approved to operate

○ A guarantee that the system is free of risk

○ A verification that a system complies with all TCSEC requirements

A is correct. The certification process includes several steps to evaluate, describe, and test a system and all of the controls that are in place to mitigate risks to the system.

B, C, and D are incorrect. Once a system is certified, an accrediting authority provides a formal declaration that the system is approved to operate, but this is the final result, not the process leading up to the certification. The certification and accreditation process does not provide a guarantee that a system is free of risk. Certification does not verify that a system complies with the rusted Computer System Evaluation Criteria (TCSEC), which has been superseded by the Common Criteria.

Question 2

1 / 1 pts

Organizations that handle any type of PHI must protect that data. What U.S. law mandates the protection of this information?

○ PCI DSS

● HIPAA

○ SOX

○ Common Criteria

B is correct. The Health Insurance Portability and Accountability Act (HIPAA) mandates protection of health-related data within the United States.

A, C, and D are incorrect. The Payment Card Industry Data Security Standard (PCI DSS) requires that organizations that process credit card payments comply with specific steps to protect customer account data. The Sarbanes-Oxley (SOX) Act of 2002 mandates specific protections for data related to publicly held companies. The Common Criteria is a framework used to evaluate systems.

Question 3

1 / 1 pts

In the context of a database, what is a view?

○ A row within a table

○ A column within at table

● A virtual table

○ A primary key

C is correct. A view is a virtual table that provides access to specific columns in one or more tables. It doesn’t actually hold any data but presents the data in the underlying table or tables. A database administrator can grant access to a view without granting access to a table to limit what a user can see and manipulate.

A, B, and D are incorrect. A tuple is a row of data within a table. Each row or tuple contains a unique data element. A column (or attribute) provides additional details on the data. A primary key is used to identify each row or tuple uniquely and ensures that each item has only a single row in a table.

Question 4

1 / 1 pts

In the context of a database, what is used to create relationships between two tables?

○ A tuple

● A foreign key

○ A virtual table

○ A view

B is correct. A foreign key provides a relationship to another table. A foreign key in one table points to a primary key in another table.

A, C, and D are incorrect. A tuple is a row of data within a table, and each row or tuple contains a unique data element. A view is a virtual table that provides access to specific columns in one or more tables.

Question 5

1 / 1 pts

Of the following choices, what must be protected to comply with legislation?

● PII

○ Internal procedures

○ Sensitive data

○ Internal policies

A is correct. Personally identifiable information (PII) is any information that can be used to distinguish or trace an individual’s identity, and many laws mandate its protection.

B, C. and D are incorrect. Sensitive data includes internal information that requires special precautions to protect, such as financial information about a company. Internal procedures are internal policies are important internally, but not protected by laws.

Question 6

1 / 1 pts

Which of the following provides the best description of data in motion?

○ Any data that is no longer being used by the organization

○ Any data that is in computer storage, such as on system hard drives, portable USB drives, flash drives, storage are networks, or backup tapes

● Any data being transmitted over a network

○ Any data encrypted with TLS or IPSec

C is correct. Data in motion (sometimes called data in transit) is any data being transmitted over a network.

A, B, and D are incorrect. Data in motion is being actively used. Data at rest is data that is in computer storage, such as on system hard drives, portable USB drives, flash drives, storage are networks, or backup tapes, and so on. Data in motion may be encrypted with an encryption protocol such as Transport Layer Security (TLS) or Internet Protocol Security (IPSec), but unencrypted data can also be data in motion.

Question 7

1 / 1 pts

An organization wants to ensure that employees know which data is important and needs higher-level protection, and which data is less important. What can the organization do to achieve these goals?

● Classify the data

○ Encrypt the data

○ Back up the data

○ Protect the data

A is correct. One of the first steps in protecting data is identifying which data needs protection by classifying it. A common classification scheme used in private organizations is to label data Confidential, Private, Sensitive, and Public.

B, C, and D are incorrect. Although encrypting, backup up, and protecting the data are all important, if data is not classified, users will make their own determinations on the importance of data, which may be different from the data’s actual importance.

Question 8

1 / 1 pts

A company has classified its data using a common classification scheme used within private organizations. Of the following choices, what most likely represents the most valuable data deserving the highest level of protection?

○ Public

○ Internal

○ Unrestricted

● Confidential

D is correct. Of the available choices, confidential data is the most sensitive data and deserves the highest level of protection. Confidential data includes proprietary information central to the operation of a company. It could include research and development information for upcoming projects as well as trade secrets for products sold by the company.

A, B, and C are incorrect. Public data is data that is either publicly available or would not cause any harm if it were publicly available. Internal data includes information that requires special precautions to protect, such as salary information. Unrestricted data is another name for public data. Note that an organization can label data in any way they choose, so one company might label their most sensitive data as Confidential while another company might label their most sensitive data as Class 5 or Class1.

Question 9

1 / 1 pts

A company has classified its data using a common classification scheme used within private organizations. Of the following choices, what most likely represents the most valuable data deserving the highest level of protection?

○ Public

○ Internal

○ Unrestricted

● Confidential

D is correct. Of the available choices, confidential data is the most sensitive data and deserves the highest level of protection. Confidential data includes proprietary information central to the operation of a company. It could include research and development information for upcoming projects as well as trade secrets for products sold by the company.

A, B, and C are incorrect. Public data is data that is either publicly available or would not cause any harm if it were publicly available. Internal data includes information that requires special precautions to protect, such as salary information. Unrestricted data is another name for public data. Note that an organization can label data in any way they choose, so one company might label their most sensitive data as Confidential while another company might label their most sensitive data as Class 5 or Class 1.

Incorrect

Question 10

0 / 1 pts

Which of the following best describes an RMF?

○ A robust framework that helps managers identify processes to manage IT systems

○ A framework used to evaluate risks

● A framework used to evaluate systems

○ A method of tracking software projects from beginning to end

B is correct. A risk management framework (RMF) is used to evaluate risks associated with systems. NIST Special Publication (SP) 800-37 provides details on one RMF.

A, C, and D are incorrect. The Control Objectives for Information and Related Technology (COBIT) is a robust framework that helps managers identify processes to manage IT systems. The Common Criteria for Information Technology Security Evaluation (commonly called Common Criteria or simply CC) is a framework used to evaluate systems. The system development lifecycle (SDLC) is a model used to track software projects from beginning to end.

Question 11

1 / 1 pts

Which of the following best describes the purpose of a BCP?

○ A BCP is part of a DRP

○ A BCP has a narrower focus than a DRP

● A BCP provides the information to keep critical functions running during a disaster

○ A BCP identifies how one or more individual systems can be recovered after a failure

C is correct. The business continuity plan (BCP) provides the information to keep critical functions running during a disaster (such as how to move critical functions to an alternate location).

A, B, and D are incorrect. A disaster recovery plan (DRP) is part of a BCP. A DRP has a narrower focus than a BCP and identifies how one or more individual systems an be recovered after a failure.

Question 12

1 / 1 pts

An organization needs to continue operations at an alternate location even if a single location suffers a catastrophic failure. The organization wants to be able to continue operations within minutes of the outage. What type of site should the organization use?

○ A cold site

○ A warm site

● A hot site

○ A gray site

C is correct. A hot site includes all of the necessary resources to take over the operations of another location in a very short period of time, sometimes within minutes.

A, B, and D are incorrect. A cold site is a building with a roof, running water, and electricity. It doesn’t include hardware, software, or personnel. A warm site is a compromise between a cold site and a hot site. There is no such thing as a gray site as an alternate location.

Question 13

1 / 1 pts

What is used to identify the impact to the organization if any business functions are lost due to any type of incident?

○ DRP

○ BCP

● BIA

○ ALE

C is correct. A business impact analysis (BIA) is part of a business continuity plan (BCP) and it identifies the impact to the organization if any business functions are lost due to any type of incident.

A, B, and D are incorrect. A disaster recovery plan (DRP) provides an organization with a plan to restore critical operations after a disaster. The BIA is an important part of the BCP, but the BCP is much broader. Annual loss expectancy (ALE) is used in a quantitative analysis of a risk assessment.

Question 14

1 / 1 pts

An organization is developing a security policy and wants to ensure tha all employees are aware of the contents. Which of the following should NOT be considered to meet this goal?

○ It should be easy to read

○ It should remind users of the contents with warning banners

○ It should include elements in training sessions

● It should ensure that the policy is no more than a single page long

D is correct. There are no specific requirements on length for security policies. It's not uncommon for a security policy to be between 10 and 50 pages for different-size organizations.

A. B, and C are incorrect. Policies should be easy to read, and it's common to remind users of the contents with warning banners and to provide training on elements of the policy.

Question 15

1 / 1 pts

Which of the following statements is accurate about a security policy?

○ Security policies are static and should not be changed once they are created

○ Security policies should be a minimum of ten pages long

● Security policies should be updated regularly, such as once a year

○ Security policies should not be accessible to regular employees

C is correct. Security policies should be updated regularly, such as once a year. If an organization’s security policy is updated, supporting policies should also be reviewed to ensure that they still provide the necessary support.

A, B, and D are incorrect. Security risks change, so security policies are not meant to be static. Security policies do not have any required minimum or maximum length, and they should be accessible to regular employees.

Incorrect

Question 16

0 / 1 pts

Which of the following statements is accurate related to a BCP?

○ The recovery point objective is derived from the maximum allowable outage time

○ The maximum allowable outage time is derived from the recovery point objective

○ The recovery time objective is derived from the maximum allowable outage time

● The maximum allowable outage time is derived from the recovery time objective

C is correct. The business impact analysis (BIA) identifies the maximum allowable outage (MAO) time and the recovery time objective (RTO) is derived from the MAO.

A, B, and D are incorrect. The BIA determines the MAO first and administrators use it to determine the RTO. The recovery point objective (RPO) is related to databases instead of time, so it is not related to the MAO.

Incorrect

Question 17

0 / 1 pts

When comparing a business continuity plan (BCP) and a disaster recovery plan (DRP), which of the following statements is true?

○ A BCP and a DRP are essentially the same thing

○ A DRP identifies how to recover one or more individual systems after a failure

○ A BCP identifies how to recover one or more individual systems after a failure

● A DRP provides the information to keep critical functions running after a disaster

B is correct. A DRP identifies how to recover one or more individual systems after a failure.

A, C, and D are incorrect. A DRP is part of the BCP, they are not the same. The BCP (not the DRP) provides the information to keep critical functions running during and after a disaster (such as which critical functions to move to an alternate location).

Question 18

1 / 1 pts

Which of the following is an accurate statement about disaster recovery?

○ Disaster recovery is the same thing as fault tolerance

● Disaster recovery and fault tolerance are not the same thing

○ Disaster recovery includes a business continuity plan

○ Disaster recovery includes a business impact analysis

B is correct. Disaster recovery and fault tolerance are not the same thing. Disaster recovery helps an organization recover after a disaster. Fault tolerance helps ensure that a system or component continues to function after a failure.

A, C, and D are incorrect. Disaster recovery and fault tolerance are not the same thing. A business continuity plan includes a disaster recovery plan, but a disaster recovery plan does not include a business continuity plan. A business continuity plan includes a business impact analysis.

Question 19

1 / 1 pts

An organization has created an acceptable use policy. How should this be communicated to users?

○ In a warning banner

○ Via email

● By requiring users to review and acknowledge the policy

○ Posted on an intranet website

C is correct. Users should have an opportunity to review the policy, and the organization should have assurances that the user did review the acceptable use policy (AUP). Organizations commonly require users to review and acknowledge these types of policies regularly, such as once a year.

A, B, and D are incorrect. The other options can be used to reinforce the policy, but should not be the only methods. They don’t provide assurances to the organization that the user has reviewed and acknowledged the policy.

Incorrect

Question 20

0 / 1 pts

An organization needs to continue operations at an alternate location if a disaster hits. It can’t afford to keep the location manned and up to date continuously but wants the location to have much of the hardware needed to support the mission. What type of site should the organization use?

● A cold site

○ A warm site

○ A hot site

○ A BCP site

B is correct. A warm site is a compromise between a cold site and a hot site. It would have more than just a building with a roof, running water, and electricity, but it wouldn’t have all the resources needed to go active within minutes.

A, C, and D are incorrect. A cold site is a building with a roof, running water, and electricity. It doesn’t include hardware, software, or personnel. A hot site includes all of the resources necessary to take over the operations of another location in a very short period of time, sometimes within minutes. There is no such thing as a business continuity plan (BCP) site as an alternate location.

Quiz Score: **16** out of 20