Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/22/2022 1:06:04 pm • Time spent: 01:56

Score: 60% Passing Score: 80%

Question 1: ✔ Correct

Your company has developed and implemented countermeasures for the greatest risks to their assets. However, there is still some risk left. What is the remaining risk called?

- ➡ Residual risk
- Exposure
- Risk
- Loss

EXPLANATION

Residual risk is the portion of risk that remains after the implementation of a countermeasure. There is almost always some residual risk.

Exposure is the vulnerability of losses from a threat agent, and risk is the likelihood of a vulnerability being exploited. A loss is the real damages to an asset that reduces its confidentiality, integrity, or availability.

REFERENCES

13.2.2 Risk Types and Tolerance Facts

q_risk_types_tol_residual_secp7.question.fex

Question 2: ✕ Incorrect

You have conducted a risk analysis to protect a key company asset. You identify the following values:

- Asset value = 400
- Exposure factor = 75
- Annualized rate of occurrence = .25

What is the annualized loss expectancy (ALE)?

- 25
- 75
- ~~100~~
- 175
- 475

EXPLANATION

To calculate the ALE, use the following formula:

Asset value (AV) x exposure factor (EF) x annualized rate of occurrence (ARO) => 400 x 75% x .25 = 75

REFERENCES

13.2.4 Analyzing Risks Facts

q_anylz_risk_ale_02_secp7.question.fex

Question 3: ✔ Correct

What is the average number of times that a specific risk is likely to be realized in a single year?

- Estimated maximum downtime
- Exposure factor
- Annualized rate of occurrence
- Annualized loss expectancy

EXPLANATION

Annualized rate of occurrence (ARO) is the average number of times that a specific risk is likely to be realized in a single year.

Annualized loss expectancy (ALE) is ARO x SLE (single loss expectancy), which is the estimated per-year loss due to exposures. Estimated maximum downtime sounds similar to maximum tolerable downtime or recovery time objective, neither of which are related to the average number of times a risk is likely to be realized. Exposure factor is the percentage of value loss that is experienced due to an exposure rather than the number of times of exposure.

REFERENCES

13.2.4 Analyzing Risks Facts

q_anylz_risk_aro_01_secp7.question.fex

Question 4: ✔ Correct

When analyzing assets, which analysis method assigns financial values to assets?

- ➡ Quantitative
- Acceptance
- Qualitative
- Transfer

EXPLANATION

Quantitative analysis assigns a financial value or assignment of real numbers and the cost required to recover from a loss to the asset.

Qualitative analysis seeks to identify costs that cannot be concretely defined using quantitative analysis. Transfer and acceptance are responses to risk; they are not risk analysis methods.

REFERENCES

13.2.4 Analyzing Risks Facts

q_anylz_risk_quantitative_secp7.question.fex

Question 5: ✔ Correct

Which of the following best defines single loss expectancy (SLE)?

- The total cost of all countermeasures associated with protecting against a given vulnerability.
- The statistical probability of a malicious event.
- The monetary value of a single employee's loss of productivity due to a successful attack.
- ➡ The total monetary loss associated with a single occurrence of a threat.

EXPLANATION

Single loss expectancy (SLE) is best defined as the total monetary loss associated with a single occurrence of a threat. The key to this definition is the term total. In other words, this encompasses all costs, including lost employee productivity, replacement hardware/software, and payroll for additional consultants. All of this must be considered when calculating the total loss.

REFERENCES

13.2.4 Analyzing Risks Facts

q_anylz_risk_sle_01_secp7.question.fex

Question 6: ✕ Incorrect

A file server with data is consider which of the following asset types?

- ~~Tangible~~
- Intangible
- Both tangible and intangible
- Neither tangible nor intangible

EXPLANATION

Assets can have both tangible and intangible components. For example, a computer that functions as a server has a tangible value associated with the replacement cost of the hardware. Intangible assets include the data on the computer, the value of the role that the computer performs within the organization, and what the computer's information is worth to a competitor or an attacker.

A tangible asset is a physical item such as a computer, storage device, or document. Such items are typically purchased.

An intangible asset is a resource that has value and may be saleable even though it is not physical or material. Intangible assets are typically more challenging to identify and evaluate.

REFERENCES

13.2.6 Business Continuity Planning Facts

q_biz_cont_asset_secp7.question.fex

Question 7: ✔ Correct

What is the primary goal of business continuity planning?

- Minimize decision-making during the development process
- Protect an organization from major computer services failure
- Maintain business operations with reduced or restricted infrastructure capabilities or resources
- Minimize the organization's risk of service delays and interruptions

EXPLANATION

The primary goal of BCP is to maintain business operations with reduced or restricted infrastructure capabilities or resources.

Minimizing the risk of service delays and interruptions is a goal of DRP. If your organization cannot provide services, it is experiencing a disaster. Minimizing decision making during the development process is not a valid goal of BCP or DRP; decisions should be made during development. The correct DRP goal is to minimize decisions during an emergency. Protecting an organization from major computer services failure is a goal of DRP, not BCP. If computer services fail, business continuity is interrupted, creating a disaster.

REFERENCES

12.1.4 Incident Response Frameworks and Management Facts

13.2.6 Business Continuity Planning Facts

q_biz_cont_bcp_01_secp7.question.fex

Question 8: ✕ Incorrect

A broken water pipe that floods the reception area would be considered which type of threat?

- Disaster
- ➡ Natural
- External
- ~~Internal~~

EXPLANATION

Natural events are those events that may reasonably be expected to occur over time. Examples are a fire or a broken water pipe.

Disasters are major events that have significant impact on an organization. Examples are tornadoes, hurricanes, and floods.

External threats are those events originating outside of the organization that typically focus on compromising the organization's information assets.

Internal threats are intentional or accidental acts by employees. Examples are theft, fraud, snooping, and unintentional data loss.

REFERENCES

13.2.6 Business Continuity Planning Facts

q_biz_cont_environ_secp7.question.fex

Question 9: ✔ Correct

When should a hardware device be replaced in order to minimize downtime?

- Only after its first failure
- Just before its MTBF is reached
- When its performance drops below 75% efficiency
- Once every year

EXPLANATION

Hardware should be replaced just before its MTBF (mean time between failures) is reached. This is the statistical average time that the device operates before experiencing its first serious failure.

Once every year is not an appropriate replacement metric, as many devices have an MTBF of 3 to 10 years or more. Waiting until a device experiences a failure does not minimize downtime. Instead, that is a scheme to minimize hardware costs by using every device until failure before replacement. Waiting for a performance efficiency drop is an ineffective solution, as most hardware failures do not provide such pre-failure symptoms.

REFERENCES

13.2.6 Business Continuity Planning Facts

q_biz_cont_mtbf_secp7.question.fex

Question 10: ✕ Incorrect

Which of the following terms describes the actual time required to successfully recover operations in the event of an incident?

- Mean time to repair (MTTR)
- Recovery time objective (RTO)
- ~~Recovery point objective (RPO)~~
- Maximum tolerable downtime (MTD)

EXPLANATION

Recovery time objective (RTO) is the actual time required to successfully recover all operations.

The mean time to repair (MTTR) is an indication of how long it would typically take to get the system back online. Recovery point objective (RPO) is a measurement of how old data is at the point that it is successfully recovered. Any data that has been lost between the RPO and the present must either be accepted as lost or reconstructed. Maximum tolerable downtime (MTD) identifies the length of time an organization can survive with a specified service, asset, or process down.

REFERENCES

13.2.6 Business Continuity Planning Facts

q_biz_cont_rto_secp7.question.fex