Module 5 Assessment (Risk, Response, and Recovery 3rd)

Due Oct 22 at 11:59pm **Points** 20 **Questions** 20 **Available** Oct 9 at 12am - Oct 24 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	19 minutes	15 out of 20

Answers will be shown after your last attempt

Score for this attempt: **15** out of 20
Submitted Oct 17 at 9:39am
This attempt took 19 minutes.

Question 1

1 / 1 pts

An organization has implemented access controls to ensure that only authorized personnel are able to access systems and data within he organization's system. What risk management strategy is the organization using to prevent the risk of a loss of confidentiality?

- Acceptance

Avoidance

Mitigation

Transference

C is correct. Risk mitigation implements controls to reduce vulnerabilities.

A, B, and D are incorrect. Risk acceptance doesn't take any action to mitigate the risk. Risk avoidance attempts to avoid the activity that results in the risk. Risk transference transfers or shares the risk with a third party.

Incorrect

Question 2

0 / 1 pts

What is the first step to take in incident response?

Preparation

Detection

Verification

Containment

A is correct. The first step in incident response is preparation.

B, C, and D are incorrect. Once an incident has been detected and verified, it's important to contain the incident as quickly as possible, but each of these steps takes place after preparation.

Incorrect

Question 3

0 / 1 pts

Which of the following equations is sometimes used to express risk?

- Risk = Threat x Vulnerability
- Risk = Mitigated Risk - Total Risk
- Risk = Likelihood + Impact
- Risk = Threat - Vulnerability

A is correct. The formula Risk = Threat x Vulnerability is commonly used to express risk. When the threat and the vulnerability are combined (a threat exploits a vulnerability), the result is a loss.

B, C, and D are incorrect. Residual risk is calculated as Total Risk - Mitigated Risk, but Mitigated Risk - Total Risk is not a valid formula. A qualitative analysis used in a risk assessment compares the likelihood and impact. Threat - Vulnerability is not a valid formula for risk.

Question 4

1 / 1 pts

An organization has taken several steps to reduce risk, but has not eliminated all risk. What is the name of the risk that remains?

- Residual risk
- Total risk
- Mitigated risk

Transferable risk

A is correct. Residual risk is the risk that remains after steps have been taken to reduce or mitigate risk.

B, C, and D are incorrect. Total risk is the combined risk to all of the organization's assets, including all the threats and vulnerabilities. Mitigated risk is the risk that has been reduced through controls. Transferable risk is risk that an organization decides to transfer or share (such as through insurance).

Incorrect

Question 5

0 / 1 pts

Which of the following is NOT an example of a threat source?

- (•) Weather event
- ( ) Employees
- ( ) Poor hardening practices
- ( ) An attacker launching a denial of service (DoS) attack.

C is correct. Poor hardening practices are a vulnerability. Systems should be hardened or made more secure from their default configuration. This includes changing defaults such as default passwords, implementing firewalls, keeping operating systems and applications up to date with patches, and more.

A, B, and D are incorrect. Weather events, employees, and attackers are all examples of potential threat sources.

Question 6

1 / 1 pts

Which of the following best describes a threat event?

- (●) Any activity or event that can result in a loss of confidentiality, integrity, or availability to a system.
- ( ) Any activity or event that protects a system from a loss of confidentiality, integrity, or availability.
- ( ) A weakness
- ( ) The potential for an attacker to attack.

A is correct. Threat events are any type of activity or event that can result in a loss of confidentiality, integrity, or availability to a system.

B, C, and D are incorrect. Controls and countermeasures protect systems. Vulnerabilities (not threats) are any weaknesses in a system, network, or infrastructure. An attacker can exploit a vulnerability by attacking, but the potential for the attack isn't the threat event.

Question 7

1 / 1 pts

Your are planning an incident response plan. What is the first step to take?

- (●) Preparation
- ( ) Detection
- ( ) Analysis
- ( ) Containment

A is correct. The first step in an incident response plan is preparation. Preparation also includes steps to take that can prevent the incident.

B, C, and D are incorrect. Detection and analysis come after preparation. Containment is included in the containment, eradication, and recover step. Last is post-incident activity.

Question 8

1 / 1 pts

Which of the following provides the best definition of risk?

- A vulnerability that can result in a loss
- A threat that can result in a loss
- The probability or likelihood of a vulnerability exploiting a threat and resulting in a loss
- The probability or likelihood of a threat exploiting a vulnerability and resulting in a loss

D is correct. A definition of a risk is the probability or likelihood of a threat exploiting a vulnerability and resulting in a loss.

A, B, and C are incorrect. A threat is any activity that can be a possible danger, and a vulnerability is a weakness, but by themselves they are not a risk. A vulnerability cannot exploit a threat.

Question 9

1 / 1 pts

A risk assessment is using a qualitative analysis. What are two key teams that the analysis is based on?

- SLE and ARO
- ARO and ALE
- Cost and assets
- Impact and likelihood

D is correct. A qualitative analysis is subjective and determines overall risk by comparing impact and likelihood.

A, B, and C are incorrect. A quantitative analysis uses numerical-based data such as monetary figures to identify the actual cost associated with a risk. It include single loss expectancy (SLE), annual rate of occurrence (ARO), and annual loss expectancy (ALE) and uses these values to compare against the cost of the control.

Question 10

1 / 1 pts

An organization has considered the risk associated with a potential fire at its business location. The organization has decided to purchase fire insurance to cover its losses if a fire occurs. What is this called?

- Risk mitigation
- Risk avoidance
- Risk transference
- Risk acceptance

C is correct. Risk transference (sometimes called risk sharing) transfers the risk to another party (such as through insurance) so that the other party (such as the insurance company) has responsibility for the risk.

A, B, and D are incorrect. Risk mitigation reduces the risk. Risk avoidance avoids the activity that introduces the risk. Risk acceptance accepts the risk and its potential losses and is commonly done when the asset value is low or if the cost to reduce the risk is higher that the value of the asset.

Question 11

1 / 1 pts

An organization has considered the risk associated with selling products via a website on the Internet. After determining that the gains don't outweigh the risk, the organization has decided that it will not sell products on the website. What is this called?

- Risk mitigation
- Risk avoidance
- Risk transference
- Risk acceptance

B is correct. Risk avoidance avoids the activity that introduces the risk.

A, C, and D are incorrect. Risk mitigation reduces the risk. Risk transference (sometimes called risk sharing) transfers the risk to another party (such as through insurance) so that the other party (such as the insurance company) has responsibility for the risk. Risk acceptance accepts the risk and its potential losses and is commonly done when the asset value is low or if the cost to reduce the risk is higher that the value of the asset.

Question 12

1 / 1 pts

An organization is performing a risk assessment. It is using a numerical-based analysis method to evaluate risk. What type of analysis is this?

- (●) Quantitative analysis
- ( ) Qualitative analysis
- ( ) Total cost of ownership analysis
- ( ) Return on investment analysis.

A is correct. A quantitative analysis uses numerical-based data such as monetary figures to identify the actual cost associated with a risk.

B, C, and D are incorrect. A qualitative analysis is subject and often simply categorizes a risk using such words as “low”, “medium”, and “high”. Total cost of ownership and return on investment help identify the cost of the control and determine whether the savings offered by the control are greater than the cost of the control.

Question 13

1 / 1 pts

You have completed a risk assessment and determined that you can purchase a control to eliminate a specific risk for $20,000. The single loss expectancy (SLE) is $2,000 and the annual rate of occurrence (ARO) is five. Is this cost justified?

- ( ) Yes, the cost of the control is less than the savings
- (●) No, the cost of the control exceeds the savings

- Yes, the cost of the control exceeds the ARO
- No, the cost of the control is less than the ARO

B is correct. The cost of the control exceeds the savings. The single loss expectancy (SLE) is $2,000 and the annual rate of occurrence (ARO) is five. The formula for annual loss expectancy (ALE) is SLE * ARO or $10,000, which is less than the cost of the control ($20,000). In other words, you would be spending $20,000 to save $10,000 or expending an additional $10,000 annually.

A, C, and D are incorrect. The cost of the control is less than the savings, but instead is more. The cost of the control is not measured against the ARO, but instead must be measured against the savings.

Question 14

1 / 1 pts

Which of the following choices is an open standard that helps an organization assess the severity of computer system security vulnerabilities?

- NIST
- (●) CVSS
- ISO
- BIA

B is correct. The Common Vulnerability Scoring System (CVSS) is an open standard that organizaiotns can use to assss the severity of computer system security vulnerabilities.

A,C, and D are incorrect. The National Institute of Standards and Technology (NIST) purblishes many documents that are freely available, but NIST is an organization, not an open standard. The International Organization for Standardization (ISO) is an organization tht publishes standards. A business impact analysis (BIA) identifies critical functions as part of a business continutity plan (BCP).

Question 15

1 / 1 pts

You are helping a small startup company implement some basic security plans and processes. One of your goals is to support the incident lifecycle. What is the first step in the incident lifecycle?

- (●) Preparation
- ( ) Detection
- ( ) Containment
- ( ) Lessons learned

A is correct. The first step in the incident lifecycle is preparation. Preparation also includes steps to take that can prevent an incident.

B, C, and D are incorrect. Detection comes after preparatoin and includes analysis and escalation. Containmaent occurs after detection, analysis, and esclation. The lessons learned step is teh last one in the incident lifecycle and includes implementation of new countermeasurs.

Question 16

1 / 1 pts

What is the first step in the incident lifecycle?

- (●) Preparation
- ( ) Detection
- ( ) Verification
- ( ) Containment

A is correct. The first step in the incident lifecycle is preparation.

B, C, and D are incorrect. Once an incident has been detected and verified, it's important to contain the incident as quickly as possible, but each of these steps takes place after preparation.

Incorrect

Question 17

0 / 1 pts

Your organizatoin has recently suffered a significant attack on one of its web servers in the DMZ. IT personnel quickly deermined that they couldn't easily fix all the problems. Security personnel removed the server for later analysis in an isolated network and IT personnel re-created the server from an image. What should be done with the knowledge gained by analyzing the removed server?

- ( ) Keep it private within the organization.
- ( ) Use it to attack the attackers.
- ( ) Share it.

Identify TTPs.

C is correct. It is appropriate to share threat intellidence (such as the knowledge gained by analyzing the server) with other entities such as law enforcement agencies.

A, B, and D are incorrect. Security Professionals do not recommend keeping the information private because it can help other organizations detect and/or block attacks. Unless it is your specific job to launch attacks, it is never appropriate to launch attacks. The knowledge gained by analyzing the server is the tactics, techniques, and procedures (TTPs) used by the attackers and the question is asking what to do with the knowledge gained by analyzing the removed server?

Incorrect

Question 18

0 / 1 pts

Your organization hosts in the DMZ a web server that is used for e-commerce. The server hosts a database used to host customer and sales data. Management previously chose to accept the risks associated with hosting the database in the DMZ. However, after a recent attack on another server, management decided that this risk is much more severe then they previously thought and they have asked for security control recommendations to reduce the risk. What does this best describe?

Avoiding the risk.

Transferring the risk.

Recasting the risk.

Mitigating the risk.

C is correct. Recasting a risk changes the severity level of the risk. In this scenario, the risk is recast from a lower-level risk to one more severe.

A, B, and D are incorrect. To avoid the risk, the organization could choose to eliminate the web server. An organization could transfer or share the risk by purchasing insurance. Security control recommendations would mitigate the risk, but only after they are implemented.

Question 19

1 / 1 pts

Security experts in your organization are performing a risk assessment using a qualitative analysis. Of the following choices, what are they most likely to focus on during this process?

- SLE and ARO
- ARO and ALE
- Cost and assets
- Impact and likelihood

D is correct. A qualitative analysis is subjective and determines overall risk by comparing impact and likelihood.

A, B, and C are incorrect. A quantitative analysis uses numerical-based data such as monetary figures to identify the actual cost associated with a risk. It includes single loss expectancy (SLE), annual rate of occurrence (ARO), and annual loss expectancy (ALE) and uses these values to compare against the cost of the control.

Question 20

1 / 1 pts

An organization is taking steps to reduce risks by implementing controls or safeguards. What is this called?

- Risk elimination
- Risk mitigation
- Residual risk
- Reducing threats

B is correct. Risk mitigation is the practice of reducing risk. The primary method of reducing risk is to reduce or eliminate vulnerabilities by implementing safeguards or controls.

A, C, and D are incorrect. Risk cannot be eliminated. Residual risk is the risk that remains after steps have been taken to mitigate risk. Controls and threats attempt to reduce vulnerabilities and/or reduce the impact of threats.

Quiz Score: **15** out of 20