

# Mid-Term Exam Review

Ⓜ Average Score

**78%**

📈 High Score

**96%**

📉 Low Score

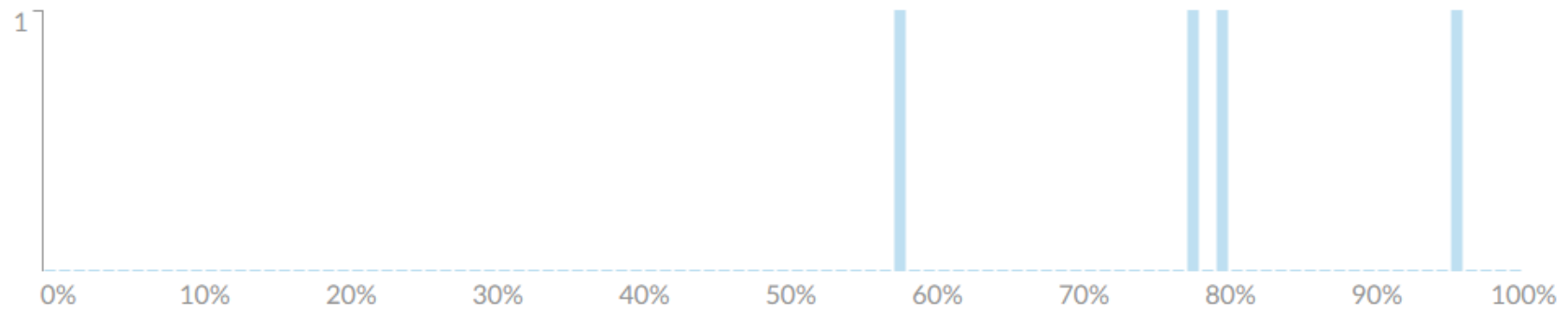
**58%**

⊖ Standard Deviation





**13.49**

🕒 Average Time





**01:15:75**







Who are responsible for ensuring that the information security policies and procedures have been adhered to?

Executive management	1 respondent	25 %	
<b>Information systems auditors</b>	1 respondent	<b>25 %</b>	
Information owners	2 respondents	50 %	
Security officers		0 %	





While auditing an e-commerce architecture, an IS auditor notes that customer master data are stored on the web server for six months after the transaction date and then purged due to inactivity. Which of the following should be the PRIMARY concern for the IS auditor?

Availability of customer data	2 respondents	50 %	
Integrity of customer data	1 respondent	25 %	
<b>Confidentiality of customer data</b>	1 respondent	<b>25 %</b>	
System storage performance		0 %	





When media is labeled based on the classification of the data it contains, what rule is typically applied regarding labels?

The media is labeled with the lowest level of classification of the data it contains		0 %	
<b>The media is labeled based on the highest classification level of the data it contains</b>	1 respondent	25 %	
The data is labeled based on its integrity requirements	1 respondent	25 %	
The media is labeled with all levels of classification of the data it contains	2 respondents	50 %	


What is a risk associated with attempting to control physical access to sensitive areas such as computer rooms using card keys or locks?

Removing access for those who are no longer authorized is complex.	2 respondents	50 %	
The contingency plan for the organization cannot effectively test controlled access practices.		0 %	
Access cards, keys and pads can be easily duplicated allowing easy compromise of the control.	1 respondent	25 %	
<b>Unauthorized individuals wait for controlled doors to open and walk in behind those authorized.</b>	1 respondent	25 %	

Which of the following choices BEST helps information owners to determine the proper security categorization of data?


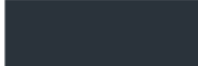
Use of an automated data leak prevention (DLP) tool		0 %	
Understanding the security controls that protect data	1 respondent	25 %	
<b>Training on organizational policies and standards</b>	2 respondents	<b>50 %</b>	 ✓
Understanding which users need to access the data	1 respondent	25 %	

A number of factors should be considered when assigning values to assets. Which of the following is not used to determine the value of an asset?

The initial and outgoing costs of purchasing, licensing, and supporting the asset		0 %	
The asset's value in the external marketplace	2 respondents	50 %	
<b>The level of insurance required to cover the asset</b>	2 respondents	50 %	 ✓
The asset's value to the organization's production operations		0 %	







Which of the following is the BEST indicator that security awareness training has been effective?

A majority of employees have received training	1 respondent	25 %	
<b>More incidents are being reported</b>	2 respondents	<b>50 %</b>	 ✓
Have employees sign to confirm they have read the security policy		0 %	
Feedback forms from training are favorable	1 respondent	25 %	

Vulnerabilities discovered during an assessment should be:

<b>Evaluated for threat, impact and cost of mitigation</b>	2 respondents	50 %	<div style="width: 50%; background-color: #2e8b57;"></div> ✓
Prioritized for remediation solely based on impact		0 %	<div style="width: 0%; background-color: #2e8b57;"></div>
Handled as a risk, even though there is no threat	2 respondents	50 %	<div style="width: 50%; background-color: #2e8b57;"></div>
A basis for analyzing the effectiveness of controls		0 %	<div style="width: 0%; background-color: #2e8b57;"></div>





Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?

Alternative power supplies	1 respondent	25 %	
Interruptible power supplies	1 respondent	25 %	
Surge protection devices		0 %	
<b>Power line conditioners</b>	2 respondents	50 %	





An IS auditor is reviewing an organization's security operation center (SOC). Which of the following choices is of greatest concern? The use of:

an uninterrupted power supply with 5 minutes of backup power.		0 %	
a wet pipe-based fire suppression system.	2 respondents	50 %	
<b>a carbon dioxide-based fire suppression system.</b>	2 respondents	<b>50 %</b>	✓
a rented rack space in the SOC.		0 %	




Which of the following is the BEST criterion for evaluating the adequacy of an organization's security awareness program?

In accordance with the degree of risk and business impact, there is adequate funding for security efforts.		0 %	
Senior management is aware of critical information assets and demonstrates an adequate concern for their protection	2 respondents	50 %	
No actual incidents have occurred that have caused a loss or a public embarrassment.		0 %	
<b>Job descriptions contain clear statements of accountability for information security.</b>	2 respondents	50 %	

Which of the following would be BEST prevented by a raised floor in the computer machine room?

A power failure from static electricity		0 %	
Shocks from earthquakes		0 %	
Water flood damage	2 respondents	50 %	
<b>Damage to wires around computers and servers</b>	2 respondents	<b>50 %</b>	 ✓

When developing a risk management program, what is the FIRST activity to be performed?

Criticality analysis		0 %	
<b>Inventory of assets</b>	2 respondents	<b>50 %</b>	 ✓
Threat assessment		0 %	
Classification of data	2 respondents	50 %	