

Mid-Term Exam Review

Quiz Summary

Ⓜ Average Score

82%

⤴ High Score

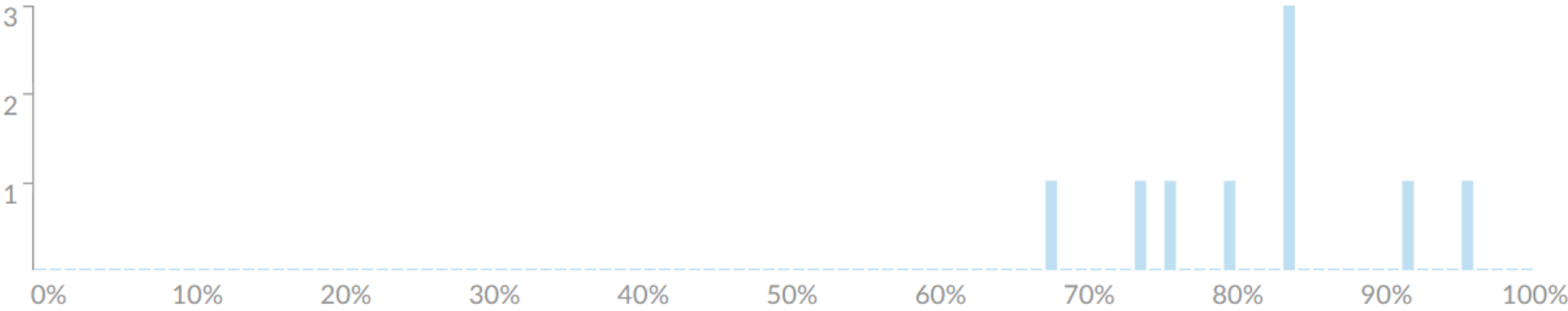
96%

⤵ Low Score



68%

⊖ Standard Deviation

8.22






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

a carbon dioxide-based fire suppression system.	1 respondent	11 %	
a wet pipe-based fire suppression system.	5 respondents	56 %	
a rented rack space in the SOC.	2 respondents	22 %	
an uninterrupted power supply with 5 minutes of backup power.	1 respondent	11 %	

The GREATEST benefit of having well-defined data categorization policies and procedures is:

An improved regulatory compliance	1 respondent	11 %	
A more accurate inventory of information assets	2 respondents	22 %	
A reduced risk of inappropriate system access	3 respondents	33 %	
A decreased cost of controls	3 respondents	33 %	

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

Information systems auditors	3 respondents	33%		✓
Executive management	2 respondents	22%		
Security officers	2 respondents	22%		
Information owners	2 respondents	22%		




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

Understanding the security controls that protect data	4 respondents	44 %	
Use of an automated data leak prevention (DLP) tool		0 %	
Understanding which users need to access the data	1 respondent	11 %	
Training on organizational policies and standards	4 respondents	44 %	

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

Power line conditioners	4 respondents	44%	✓
Alternative power supplies	1 respondent	11%	
Surge protection devices		0%	
Interruptible power supplies	4 respondents	44%	





Which of the following exposures associated with the spooling of sensitive reports for offline printing should an IS auditor consider to be the MOST serious?

Unauthorized report copies can be printed	5 respondents	56 %	 ✓
Data can be amended without authorization	1 respondent	11 %	
Sensitive data can be read by operators	3 respondents	33 %	
Output can be lost in the event of system failure		0 %	





Which statement below best describes the purpose of risk analysis?

To influence the system design process		0 %	
To develop a clear cost-to-value reason for implementing security controls	3 respondents	33 %	
To influence site selection decisions	1 respondent	11 %	
To quantify the impact of potential threats	5 respondents	56 %	✓

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

Shocks from earthquakes		0 %	
Water flood damage	3 respondents	33 %	
A power failure from static electricity	1 respondent	11 %	
Damage to wires around computers and servers	5 respondents	56 %	 ✓

Information such as data that is critical to a company needs to be properly identified and classified. In general, what are the guidelines to classify data?

Classify only data that is digital in nature and exists on the company servers, desktops and all computers in the company		0 %	
Classify all data irrespective of the format it exists in (paper, digital, audio, video)	6 respondents	67 %	 ✓
Classify only data that is digital in nature and exists on the company servers	1 respondent	11 %	
Classify all data irrespective of format (digital, audio, video) excluding paper	2 respondents	22 %	

Vulnerabilities discovered during an assessment should be:

Evaluated for threat, impact and cost of mitigation	6 respondents	67%	✓
Handled as a risk, even though there is no threat	2 respondents	22%	
Prioritized for remediation solely based on impact	1 respondent	11%	
A basis for analyzing the effectiveness of controls		0%	

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

Job descriptions contain clear statements of accountability for information security.	6 respondents	67 %	<input checked="" type="checkbox"/>
No actual incidents have occurred that have caused a loss or a public embarrassment.	1 respondent	11 %	
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	22 %	

Next steps...

- Review your exam results in Canvas
- Study the questions you answered incorrectly
- If you have any remaining questions, schedule an appointment and meet with Professor Lanter to discuss