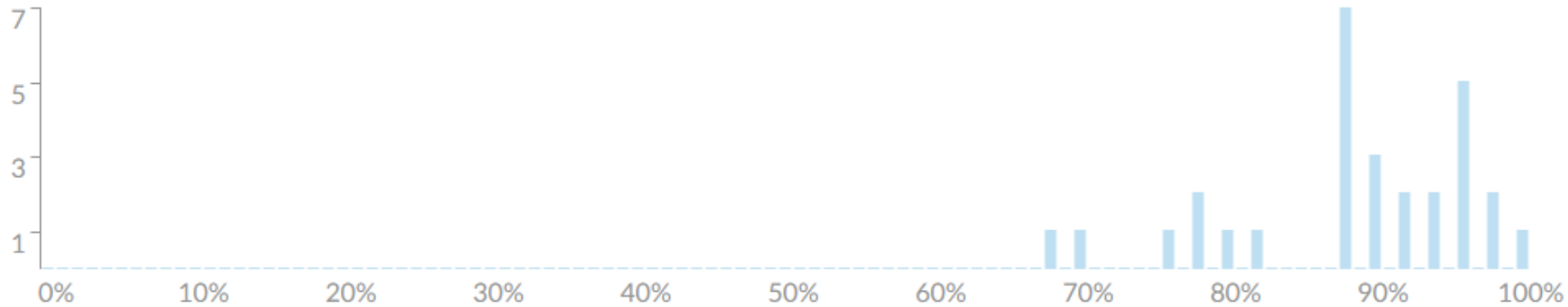
MIS 5206 Section 701

Mid-term Exam Review

Average Score	High Score	Low Score	Standard Deviation	Average Time
88%	100%	68%	8.18	01:16:44



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

Information owners	12 respondents	41 %	
Information systems auditors	10 respondents	**34 %**	
Executive management	4 respondents	14 %	
Security officers	3 respondents	10 %	

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 rented rack space in the SOC.	6 respondents	21 %	
a carbon dioxide-based fire suppression system.	14 respondents	**48 %**	
an uninterrupted power supply with 5 minutes of backup power.	4 respondents	14 %	
a wet pipe-based fire suppression system.	5 respondents	17 %	

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, their is adequate funding for security efforts.	1 respondent	3 %	
Job descriptions contain clear statements of accountability for information security.	17 respondents	**59 %**	
No actual incidents have occurred that have caused a loss or a public embarrassment.	3 respondents	10 %	
Senior management is aware of critical information assets and demonstrates an adequate concern for their protection	8 respondents	28 %	

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?

Integrity of customer data	7 respondents	24 %	
System storage performance		0 %	
Confidentiality of customer data	18 respondents	**62 %**	
Availability of customer data	4 respondents	14 %	

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

A power failure from static electricity	1 respondent	3 %
Damage to wires around computers and servers	21 respondents	**72 %**
Water flood damage	7 respondents	24 %
Shocks from earthquakes		0 %

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

Interruptible power supplies	2 respondents	7 %	
Alternative power supplies	3 respondents	10 %	
Power line conditioners	22 respondents	**76 %**	
Surge protection devices	2 respondents	7 %	

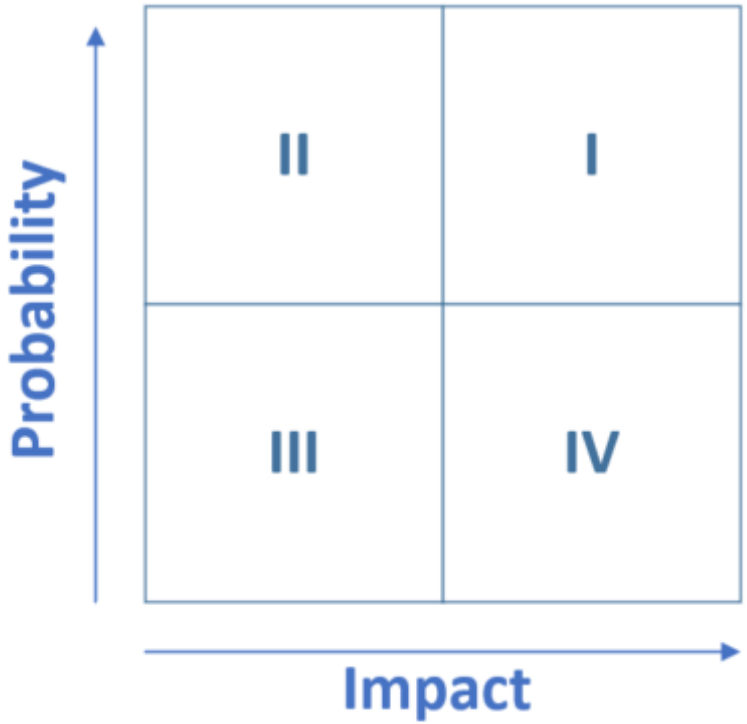
Which best describes the difference between a system owner and an information owner?

The information owner is responsible for defining a system's operating parameters	3 respondents	10 %
A system owner is responsible for defining the rules for the use of information	3 respondents	10 %
One system could have multiple information owners	23 respondents	**79 %**
There is a 1:1 relationship between system and information owners		0 %

When helping an organization understand the business context of information resources that support critical functions and the cyber security risks they face, the team should first create a list of information assets. What should happen next?

Develop a value for each asset	23 respondents	**79 %**	
Identify threats facing each asset	5 respondents	17 %	
Determine the risks facing the asset	1 respondent	3 %	
Identify vulnerabilities in each asset		0 %	

Lanter Industries' risk assessment team recently conducted a qualitative risk assessment and develop a matrix similar to the one shown here.



Which quadrant of the matrix contains risks that require the most immediate attention?

III	1 respondent	3 %
II	2 respondents	7 %
IV	3 respondents	10 %
I	23 respondents	**79 %** ✓