# GIAC
# GSTRT
## GIAC Strategic Planning, Policy, and Leadership (GSTRT)

**For More Information – Visit link below:**
**https://www.examsempire.com/**

**Product Version**

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

# Latest Version: 6.1

## Question: 1

Your organization is in the process of developing a security program to meet new regulatory requirements. The program must be rolled out across multiple global offices. Several regional managers are concerned that the new security controls may hinder business operations in their specific markets. How would you address these concerns while ensuring compliance with the regulations?
Response:

A. Ignore the regional managers and implement the same controls across all offices
B. Work with the regional managers to customize the security controls where possible to meet local market needs, while still ensuring that the overall program complies with regulatory requirements
C. Delay the rollout until all managers agree
D. Eliminate security controls that impact business operations

**Answer: B**

## Question: 2

What is the primary purpose of conducting a threat modeling exercise in an organization?
Response:

A. To ignore the organization's existing security measures
B. To identify potential threats, vulnerabilities, and countermeasures specific to the organization’s assets and systems
C. To replace the risk assessment process
D. To delay the deployment of new security technologies

**Answer: B**

## Question: 3

Which communication skill is most important for a leader to possess when addressing a diverse, multi-disciplinary cybersecurity team?
Response:

A. Delegation
B. Active listening
C. Persuasion
D. Time management

**Answer: B**

## Question: 4

Your organization has been monitoring an increasing number of phishing attacks targeting senior leadership. You've identified several incidents where executives nearly fell victim to these scams. What steps should you take to mitigate this specific threat?
Response:

A. Disable all email accounts to prevent phishing attacks
B. Implement targeted phishing awareness training for executives, deploy email filtering and anti-phishing technologies, and establish multi-factor authentication for sensitive accounts
C. Assume that executives will eventually fall victim and focus on remediation
D. Ignore the threat since no successful attacks have occurred yet

**Answer: B**

## Question: 5

What is the best method to provide constructive feedback to a cybersecurity team member after a project failure?
Response:

A. Highlight only the mistakes made during the project
B. Schedule a private meeting, focus on areas for improvement, and offer actionable suggestions
C. Send an email summarizing their mistakes and ask them to do better next time
D. Discuss their mistakes during a team meeting to provide a learning opportunity for others

**Answer: B**

## Question: 6

Why is it important for an organization to understand the motivations of different types of threat actors?
Response:

A. To hire threat actors as consultants
B. To tailor its cybersecurity strategy to address the specific threats posed by different actors, such as cybercriminals, nation-states, or hacktivists
C. To avoid implementing too many security controls
D. To limit investment in security technologies

**Answer: B**

## Question: 7

Which of the following is a key business driver that should influence a cybersecurity strategy?
Response:

A. The personal preferences of the security team
B. Regulatory compliance requirements that the organization must meet
C. Reducing the number of security policies
D. The organization's desire to reduce its workforce

**Answer: B**

## Question: 8

When managing cybersecurity policies, what is the most effective way to handle outdated policies?
Response:

A. Archive the policy and never review it
B. Update the policy based on current security threats, technologies, and regulations
C. Remove the policy from circulation without review
D. Continue enforcing the outdated policy to maintain consistency

**Answer: B**

## Question: 9

Your organization is preparing to roll out a new Bring Your Own Device (BYOD) policy to allow employees to use personal devices for work purposes. The IT team is concerned about the potential security risks associated with this policy. How would you address these concerns while ensuring the policy aligns with business objectives?
Response:

A. Implement the policy without addressing security concerns, as BYOD aligns with business goals
B. Collaborate with the IT team to establish clear security guidelines, including device encryption, regular security updates, and remote wiping in case of loss, and communicate these requirements in the policy
C. Restrict the use of personal devices and require all employees to use company-provided devices
D. Delay the policy implementation until the IT team has fully assessed all risks

**Answer: B**

## Question: 10

When analyzing the business environment to inform a cybersecurity strategy, why is it important to consider the organization's competitive landscape?
Response:

A. To ensure cybersecurity measures are more expensive than those of competitors
B. To understand industry-specific risks and align security strategies with the organization's position in the market
C. To ignore cybersecurity and focus on market share
D. To prevent collaboration with business leaders

**Answer: B**

# Thank You for Trying Our Product

**Special 16 USD Discount Coupon: NSZUBG3X**

**Email:** support@examsempire.com

**Check our Customer Testimonials and ratings available on every product page.**

**Visit our website.**

**https://examsempire.com/**