Download PECB NIS-2-Directive-Lead-Implementer Exam Dumps Free

Shared by Porter on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the requirement for Member States regarding resources for competent authorities and single points of contact under Article 8 of the NIS 2 Directive?

Options:

A- To provide unlimited resources for any related tasks
B- To provide adequate resources for efficient execution of tasks and the Directive's objectives
C- To allocate resources solely for international cooperation

Answer:

B

Question 2

Question Type: MultipleChoice

During which phase of the key management life cycle can keys be manually adjusted to implement alternative algorithms?

Options:

A- Key generation
B- Key backup or recovery
C- Key rotation

Answer:

C

Question 3

Question Type: MultipleChoice

Scenario 4: StellarTech is a technology company that provides innovative solutions for a connected world. Its portfolio includes groundbreaking Internet of Things (IoT) devices, high-

performance software applications, and state-of-the-art communication systems. In response to the ever-evolving cybersecurity landscape and the need to ensure digital resilience, StellarTech has decided to establish a cybersecurity program based on the NIS 2 Directive requirements. The company has appointed Nick, an experienced information security manager, to ensure the successful implementation of these requirements. Nick initiated the implementation process by thoroughly analyzing StellarTech's organizational structure. He observed that the company has embraced a well-defined model that enables the allocation of verticals based on specialties or operational functions and facilitates distinct role delineation and clear responsibilities.

To ensure compliance with the NIS 2 Directive requirements, Nick and his team have implemented an asset management system and established as asset management policy, set objectives, and the processes to achieve those objectives. As part of the asset management process, the company will identify, record, maintain all assets within the system's scope.

To manage risks effectively, the company has adopted a structured approach involving the definition of the scope and parameters governing risk management, risk assessments, risk treatment, risk acceptance, risk communication, awareness and consulting, and risk monitoring and review processes. This approach enables the application of cybersecurity practices based on previous and currently cybersecurity activities, including lessons learned and predictive indicators. StellarTech's organization-wide risk management program aligns with objectives monitored by senior executives, who treat it like financial risk. The budget is structured according to the risk landscape, while business units implement executive vision with a strong awareness of system-level risks. The company shares real-time information, understanding its role within the larger ecosystem and actively contributing to risk understanding. StellarTech's agile response to evolving threats and emphasis on proactive communication showcase its dedication to cybersecurity excellence and resilience.

Last month, the company conducted a comprehensive risk assessment. During this process, it identified a potential threat associated with a sophisticated form of cyber intrusion, specifically targeting IoT devices. This threat, although theoretically possible, was deemed highly unlikely to materialize due to the company's robust security measures, the absence of prior incidents, and its existing strong cybersecurity practices.

Based on the scenario above, answer the following question:

What organizational model has StellarTech embraced?

Options:

A- Divisional
B- Matrix
C- Functional

Answer:

C

Question 4

Question Type: MultipleChoice

Which of the following is a recommended practice to improve cybersecurity awareness?

Options:

A- Evaluating cybersecurity behavior
B- Implementing a one-size-fits-all cybersecurity awareness plan for all organizations
C- Employing advanced technologies for performing critical processes

Answer:

A

Question 5

Question Type: MultipleChoice

Scenario 2:

MHospital, founded in 2005 in Metropolis, has become a healthcare industry leader with over 2,000 dedicated employees known for its commitment to qualitative medical services and patient care innovation. With the rise of cyberattacks targeting healthcare institutions, MHospital acknowledged the need for a comprehensive cyber strategy to mitigate risks effectively and ensure patient safety and data security. Hence, it decided to implement the NIS 2 Directive requirements. To avoid creating additional processes that do not fit the company's context and culture, MHospital decided to integrate the Directive's requirements into its existing processes. To initiate the implementation of the Directive, the company decided to conduct a gap analysis to assess the current state of the cybersecurity measures against the requirements outlined in the NIS 2 Directive and then identify opportunities for closing the gap.

Recognizing the indispensable role of a computer security incident response team (CSIRT) in maintaining a secure network environment, MHospital empowers its CSIRT to conduct thorough penetration testing on the company's networks. This rigorous testing helps identify vulnerabilities with a potentially significant impact and enables the implementation of robust security measures. The CSIRT monitors threats and vulnerabilities at the national level and assists MHospital regarding real-time monitoring of their network and information systems. MHospital also conducts cooperative evaluations of security risks within essential supply chains for critical ICT services and systems. Collaborating with interested parties, it engages in the assessment of

security risks, contributing to a collective effort to enhance the resilience of the healthcare sector against cyber threats.

To ensure compliance with the NIS 2 Directive's reporting requirements, MHospital has streamlined its incident reporting process. In the event of a security incident, the company is committed to issuing an official notification within four days of identifying the incident to ensure that prompt actions are taken to mitigate the impact of incidents and maintain the integrity of patient data and healthcare operations. MHospital's dedication to implementing the NIS 2 Directive extends to cyber strategy and governance. The company has established robust cyber risk management and compliance protocols, aligning its cybersecurity initiatives with its overarching business objectives.

Based on scenario 2, in order to avoid creating additional processes that do not fit with the company's context and culture, MHospital decided to integrate the Directive's requirements into its existing processes. Is this in accordance with best practices?

Options:

A- Yes, organizations should incorporate the NIS 2 Directive into their existing processes
B- No, organizations should create other processes in addition to the existing processes to ensure full compliance with the NIS 2 Directive
C- No, organizations should disregard existing processes completely and create new ones to ensure full compliance with the NIS 2 Directive

Answer:

A

Question 6

Question Type: MultipleChoice

What should a cybersecurity policy specify with regard to the handling of sensitive information?

Options:

A- Guidelines explaining how to permanently delete all sensitive data
B- Guidelines on sharing permissions and data masking techniques during threats
C- Guidance on sharing sensitive information on social media platforms

Answer:

B

Question 7

Question Type: MultipleChoice

What is the key difference between Tier 2 and Tier 3 disaster recovery strategies?

Options:

A- Tier 2 involves electronic vaulting of critical data, while Tier 3 relies on offsite vaults
B- Tier 2 uses couriers to transport data between centers, while Tier 3 uses electronic vaulting of critical data
C- Tier 2 mandates dual sites with peer-to-peer connections, whereas Tier 3 focuses on data transfer enhancement

Answer:

B