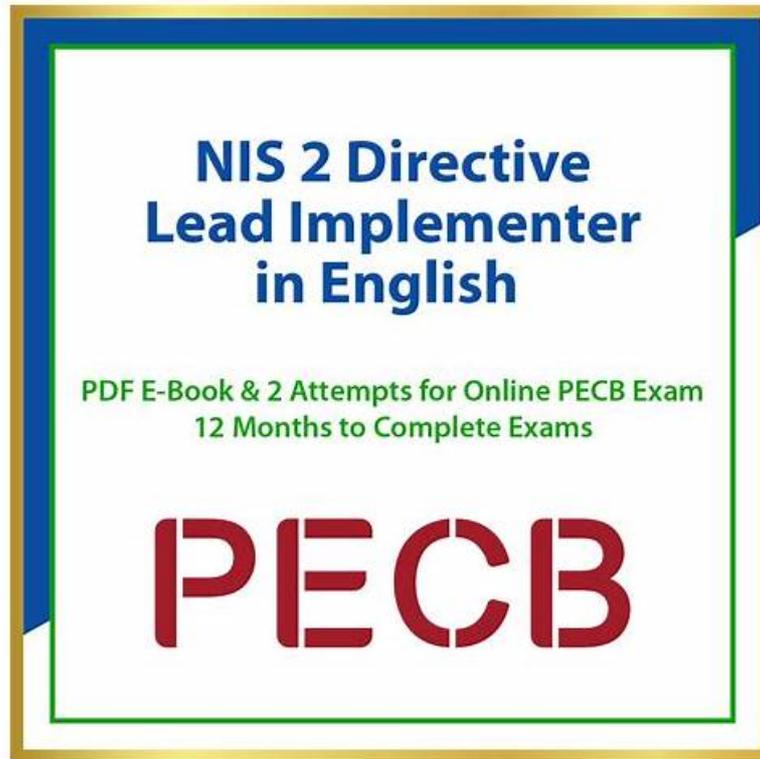


Pass Guaranteed PECB - NIS-2-Directive-Lead-Implementer Pass-Sure PDF



2026 Latest Pass4SureQuiz NIS-2-Directive-Lead-Implementer PDF Dumps and NIS-2-Directive-Lead-Implementer Exam Engine Free Share: https://drive.google.com/open?id=10HgGCRFGb5dzoCnojXSKBX7zf_CcRIKF

As is known to us, different people different understanding of learning, and also use different methods in different periods, and different learning activities suit different people, at different times of the day. Our NIS-2-Directive-Lead-Implementer test questions are carefully designed by a lot of experts and professors in order to meet the needs of all customers. We can promise that our NIS-2-Directive-Lead-Implementer Exam Question will be suitable for all people, including student, housewife, and worker and so on. No matter who you are, you must find that our NIS-2-Directive-Lead-Implementer guide torrent will help you pass the NIS-2-Directive-Lead-Implementer exam easily.

PECB NIS-2-Directive-Lead-Implementer Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">Planning of NIS 2 Directive requirements implementation: This domain targets Project Managers and Implementation Specialists focusing on how to initiate and plan the rollout of NIS 2 Directive requirements. It includes using best practices and methodologies to align organizational processes and cybersecurity programs with the directive's mandates.
Topic 2	<ul style="list-style-type: none">Testing and monitoring of a cybersecurity program: This domain assesses the abilities of Security Auditors and Compliance Officers in testing and monitoring the effectiveness of cybersecurity programs. Candidates learn to design and conduct audits, continuous monitoring, performance measurement, and apply continual improvement practices to maintain NIS 2 Directive compliance.
Topic 3	<ul style="list-style-type: none">Cybersecurity roles and responsibilities and risk management: This section measures the expertise of Security Leaders and Risk Managers in defining and managing cybersecurity roles and responsibilities. It also covers comprehensive risk management processes, including identifying, assessing, and mitigating cybersecurity risks in line with NIS 2 requirements.

Hot NIS-2-Directive-Lead-Implementer PDF - Updated & Authoritative NIS-2-Directive-Lead-Implementer Materials Free Download for PECB NIS-2-Directive-Lead-Implementer Exam

A free trial of the product allows users to test the material before buying. These different formats allow NIS-2-Directive-Lead-Implementer exam aspirants to practice using their preferred method. The support offered by the Pass4SureQuiz is another significant advantage for applicants. The Pass4SureQuiz NIS-2-Directive-Lead-Implementer provides 24/7 support for guidance of users. Our team of professionals is highly qualified and have years of experience in the industry. They are available to answer any PECB NIS-2-Directive-Lead-Implementer Questions that customers may have. The support team is always available to help applicants use the product.

PECB Certified NIS 2 Directive Lead Implementer Sample Questions (Q19-Q24):

NEW QUESTION # 19

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 scenario 4, which framework is StellarTech's structured approach to managing risks aligned with?

- A. COSO ERM Framework
- B. ENISA Risk Management Framework
- C. ISO 31000

Answer: C

NEW QUESTION # 20

Scenario 1:

into incidents that could result in substantial material or non-material damage. When it comes to identifying and mitigating risks, the company has employed a standardized methodology. It conducts thorough risk identification processes across all operational levels, deploys mechanisms for early risk detection, and adopts a uniform framework to ensure a consistent and effective incident response. In alignment with its incident reporting plan, SecureTech reports on the initial stages of potential incidents, as well as after the successful mitigation or resolution of the incidents.

Moreover, SecureTech has recognized the dynamic nature of cybersecurity, understanding the rapid technological evolution. In

response to the ever-evolving threats and to safeguard its operations, SecureTech took a proactive approach by implementing a comprehensive set of guidelines that encompass best practices, effectively safeguarding its systems, networks, and data against threats. The company invested heavily in cutting-edge threat detection and mitigation tools, which are continuously updated to tackle emerging vulnerabilities. Regular security audits and penetration tests are conducted by third-party experts to ensure robustness against potential breaches. The company also prioritizes the security of customers' sensitive information by employing encryption protocols, conducting regular security assessments, and integrating multi-factor authentication across its platforms. SecureTech reports on the initial stages of potential incidents and after the successful mitigation or resolution of the incidents. Is this in compliance with the NIS 2 Directive requirements? Refer to scenario 1.

- A. Yes, the Directive introduces a two-stage approach to incident reporting, requiring initial and final reports.
- B. No, the Directive requires that incidents are reported only in their initial stages
- C. No, the Directive requires that incidents are reported only after they have been resolved

Answer: A

NEW QUESTION # 21

Scenario 3: Founded in 2001, SafePost is a prominent postal and courier company headquartered in Brussels, Belgium. Over the years, it has become a key player in the logistics and courier in the region. With more than 500 employees, the company prides itself on its efficient and reliable services, catering to individual and corporate clients. SafePost has recognized the importance of cybersecurity in an increasingly digital world and has taken significant steps to align its operations with regulatory directives, such as the NIS 2 Directive.

SafePost recognized the importance of thoroughly analyzing market forces and opportunities to inform its cybersecurity strategy. Hence, it selected an approach that enabled the analysis of market forces and opportunities in the four following areas: political, economic, social, and technological. The results of the analysis helped SafePost in anticipating emerging threats and aligning its security measures with the evolving landscape of the postal and courier industry.

To comply with the NIS 2 Directive requirements, SafePost has implemented comprehensive cybersecurity measures and procedures, which have been documented and communicated in training sessions. However, these procedures are used only on individual initiatives and have still not been implemented throughout the company. Furthermore, SafePost's risk management team has developed and approved several cybersecurity risk management measures to help the company minimize potential risks, protect customer data, and ensure business continuity.

Additionally, SafePost has developed a cybersecurity policy that contains guidelines and procedures for safeguarding digital assets, protecting sensitive data, and defining the roles and responsibilities of employees in maintaining security. This policy will help the company by providing a structured framework for identifying and mitigating cybersecurity risks, ensuring compliance with regulations, and fostering a culture of security awareness among employees, ultimately enhancing overall cybersecurity posture and reducing the likelihood of cyber incidents.

As SafePost continues to navigate the dynamic market forces and opportunities, it remains committed to upholding the highest standards of cybersecurity to safeguard the interests of its customers and maintain its position as a trusted leader in the postal and courier industry.

Based on scenario 3, what is the level of process maturity of SafePost?

- A. Initial
- B. Defined
- C. Managed

Answer: A

NEW QUESTION # 22

Scenario 6: Solicure is a leading pharmaceutical company dedicated to manufacturing and distributing essential medications. Thriving in an industry characterized by strict regulations and demanding quality benchmarks, Solicure has taken proactive steps to adhere to the requirements of the NIS 2 Directive. This proactive approach strengthens digital resilience and ensures the continued excellence of product offerings.

Last year, a cyberattack disrupted Solicure's research and development operations, raising concerns about the potential compromise of sensitive information regarding drug formulation. Solicure initiated an immediate investigation led by its cybersecurity team, gathering technical data to understand the attackers' methods, assess the damage, and swiftly identify the source of the breach. In addition, the company implemented measures to isolate compromised systems and remove the attackers from its network. Lastly, acknowledging the necessity for long-term security improvement, Solicure implemented a comprehensive set of security measures to comply with NIS 2 Directive requirements, covering aspects such as cybersecurity risk management, supply chain security, incident handling, crisis management, and cybersecurity crisis response planning, among others.

In line with its crisis management strategy, Solicure's chief information security officer, Sarah, led the initiative to develop a comprehensive exercise plan to enhance cyber resilience. This plan was designed to be adaptable and inclusive, ensuring that organizational decision-makers possessed the essential knowledge and skills required for effective cybersecurity threat mitigation. Additionally, to enhance the efficacy of its crisis management planning, Solicure adopted an approach that prioritized the structuring of crisis response.

A key aspect of Solicure's cybersecurity risk management approach centered on the security of its human resources. Given the sensitive nature of its pharmaceutical products, the company placed utmost importance on the employees' backgrounds. As a result, Solicure implemented a rigorous evaluation process for new employees, including criminal history reviews, prior role investigations, reference check, and pre-employment drug tests.

To comply with NIS 2 requirements, Solicure integrated a business continuity strategy into its operations. As a leading provider of life-saving medicines and critical healthcare products, Solicure faced high stakes, with potential production and distribution interruptions carrying life-threatening consequences for patients. After extensive research and consultation with business management experts, the company decided to utilize a secondary location to reinforce the critical operations at the primary site. Along with its business continuity management strategy, Solicure developed a set of procedures to recover and protect its IT infrastructure in the event of a disaster and ensure the continued availability of its medications.

Which of the following crisis management planning approaches did Solicure adopt? Refer to scenario 6.

- A. Resource-based approach
- B. Resilience-based approach
- C. Crisis-driven approach

Answer: C

NEW QUESTION # 23

Scenario 3: Founded in 2001, SafePost is a prominent postal and courier company headquartered in Brussels, Belgium. Over the years, it has become a key player in the logistics and courier in the region. With more than 500 employees, the company prides itself on its efficient and reliable services, catering to individual and corporate clients. SafePost has recognized the importance of cybersecurity in an increasingly digital world and has taken significant steps to align its operations with regulatory directives, such as the NIS 2 Directive.

SafePost recognized the importance of thoroughly analyzing market forces and opportunities to inform its cybersecurity strategy. Hence, it selected an approach that enabled the analysis of market forces and opportunities in the four following areas: political, economic, social, and technological. The results of the analysis helped SafePost in anticipating emerging threats and aligning its security measures with the evolving landscape of the postal and courier industry.

To comply with the NIS 2 Directive requirements, SafePost has implemented comprehensive cybersecurity measures and procedures, which have been documented and communicated in training sessions. However, these procedures are used only on individual initiatives and have still not been implemented throughout the company. Furthermore, SafePost's risk management team has developed and approved several cybersecurity risk management measures to help the company minimize potential risks, protect customer data, and ensure business continuity.

Additionally, SafePost has developed a cybersecurity policy that contains guidelines and procedures for safeguarding digital assets, protecting sensitive data, and defining the roles and responsibilities of employees in maintaining security. This policy will help the company by providing a structured framework for identifying and mitigating cybersecurity risks, ensuring compliance with regulations, and fostering a culture of security awareness among employees, ultimately enhancing overall cybersecurity posture and reducing the likelihood of cyber incidents.

As SafePost continues to navigate the dynamic market forces and opportunities, it remains committed to upholding the highest standards of cybersecurity to safeguard the interests of its customers and maintain its position as a trusted leader in the postal and courier industry.

Based on the scenario above, answer the following question:

Why does the NIS 2 Directive apply to SafePost?

- A. Because the directive applies only to companies with more than 500 employees that provide postal services within the European Union
- B. Because the directive applies to entities that offer trust services as defined by EU regulations within the European Union
- C. Because the directive applies to companies that provide postal services within the European Union

Answer: C

NEW QUESTION # 24

.....

