

NIS-2-Directive-Lead-Implementer Test Prep Like the Real Exam Questions Can Help You Pass NIS-2-Directive-Lead-Implementer Exam - ExamsReviews



DOWNLOAD the newest ExamsReviews NIS-2-Directive-Lead-Implementer PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1tjg7EhTL3nINJPY5ePb1LlPR_lcGfPCx

No doubt the PECB Certified NIS 2 Directive Lead Implementer (NIS-2-Directive-Lead-Implementer) certification is one of the most challenging certification exams in the market. This PECB Certified NIS 2 Directive Lead Implementer (NIS-2-Directive-Lead-Implementer) certification exam gives always a tough time to PECB Certified NIS 2 Directive Lead Implementer (NIS-2-Directive-Lead-Implementer) exam candidates. The ExamsReviews understands this hurdle and offers recommended and real PECB NIS-2-Directive-Lead-Implementer Exam Practice questions in three different formats. These formats hold high demand in the market and offer a great solution for quick and complete PECB Certified NIS 2 Directive Lead Implementer (NIS-2-Directive-Lead-Implementer) exam preparation.

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

Topic	Details
Topic 1	<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 2	<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 3	<ul style="list-style-type: none"> Cybersecurity controls, incident management, and crisis management: This domain focuses on Security Operations Managers and Incident Response Coordinators and involves implementing cybersecurity controls, managing incident response activities, and handling crisis situations. It ensures organizations are prepared to prevent, detect, respond to, and recover from cybersecurity incidents effectively.
Topic 4	<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.

Free Download NIS-2-Directive-Lead-Implementer Examcollection Dumps Torrent & High-quality Reliable NIS-2-Directive-Lead-Implementer Test Guide Ensure You a High Passing Rate

This certification gives us more opportunities. Compared with your colleagues around you, with the help of our NIS-2-Directive-Lead-Implementer preparation questions, you will also be able to have more efficient work performance. Our NIS-2-Directive-Lead-Implementer study materials can bring you so many benefits because they have the following features. I hope you can use a cup of coffee to learn about our NIS-2-Directive-Lead-Implementer training engine. Perhaps this is the beginning of your change.

PECB Certified NIS 2 Directive Lead Implementer Sample Questions (Q77-Q82):

NEW QUESTION # 77

Which type of vulnerability assessment scans is primarily focused on evaluating websites and mobile applications of known software vulnerabilities and incorrect configurations?

- A. Application scans
- B. Web-based scans
- C. Network-based scans

Answer: A

NEW QUESTION # 78

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 an 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, what will StellarTech identify, record, and maintain during asset management?

- A. An asset framework
- B. An asset management plan
- C. An asset portfolio

Answer: A

NEW QUESTION # 79

Scenario 8: FoodSafe Corporation is a well-known food manufacturing company in Vienna, Austria, which specializes in producing

diverse products, from savory snacks to artisanal desserts. As the company operates in regulatory environment subject to this NIS 2 Directive, FoodSafe Corporation has employed a variety of techniques for cybersecurity testing to safeguard the integrity and security of its food production processes.

To conduct an effective vulnerability assessment process, FoodSafe Corporation utilizes a vulnerability assessment tool to discover vulnerabilities on network hosts such as servers and workstations. Additionally, FoodSafe Corporation has made a deliberate effort to define clear testing objectives and obtain top management approval during the discovery phase. This structured approach ensures that vulnerability assessments are conducted with clear objectives and that the management team is actively engaged and supports the assessment process, reinforcing the company's commitment to cybersecurity excellence.

In alignment with the NIS 2 Directive, FoodSafe Corporation has incorporated audits into its core activities, starting with an internal assessment followed by an additional audit conducted by its partners. To ensure the effectiveness of these audits, the company meticulously identified operational sectors, procedures, and policies. However, FoodSafe Corporation did not utilize an organized audit timetable as part of its internal compliance audit process. While FoodSafe's Corporation organizational chart does not clearly indicate the audit team's position, the internal audit process is well-structured. Auditors familiarize themselves with established policies and procedures to gain a comprehensive understanding of their workflow. They engage in discussions with employees further to enhance their insights, ensuring no critical details are overlooked.

Subsequently, FoodSafe Corporation's auditors generate a comprehensive report of findings, serving as the foundation for necessary changes and improvements within the company. Auditors also follow up on action plans in response to nonconformities and improvement opportunities.

The company recently expanded its offerings by adding new products and services, which had an impact on its cybersecurity program. This required the cybersecurity team to adapt and ensure that these additions were integrated securely into their existing framework. FoodSafe Corporation commitment to enhancing its monitoring and measurement processes to ensure product quality and operational efficiency. In doing so, the company carefully considers its target audience and selects suitable methods for reporting monitoring and measurement results. This includes incorporating additional graphical elements and labeling of endpoints in their reports to provide a clearer and more intuitive representation of data, ultimately facilitating better decision-making within the organization.

Based on scenario 8, did FoodSafe Corporation define the discovery phase of penetration testing according to NIST SP 800-115?

- A. No, the discovery phase is the process of identifying any possible attack by attempting to exploit vulnerabilities
- B. No, in the discovery phase the testing is initiated and a vulnerability analysis is conducted
- C. Yes, the discovery phase is correctly defined

Answer: C

NEW QUESTION # 80

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?

- A. Functional
- B. Divisional
- C. Matrix

Answer: A

NEW QUESTION # 81

Scenario 8: FoodSafe Corporation is a well-known food manufacturing company in Vienna, Austria, which specializes in producing diverse products, from savory snacks to artisanal desserts. As the company operates in regulatory environment subject to this NIS 2 Directive, FoodSafe Corporation has employed a variety of techniques for cybersecurity testing to safeguard the integrity and security of its food production processes.

To conduct an effective vulnerability assessment process, FoodSafe Corporation utilizes a vulnerability assessment tool to discover vulnerabilities on network hosts such as servers and workstations. Additionally, FoodSafe Corporation has made a deliberate effort to define clear testing objectives and obtain top management approval during the discovery phase. This structured approach ensures that vulnerability assessments are conducted with clear objectives and that the management team is actively engaged and supports the assessment process, reinforcing the company's commitment to cybersecurity excellence.

In alignment with the NIS 2 Directive, FoodSafe Corporation has incorporated audits into its core activities, starting with an internal assessment followed by an additional audit conducted by its partners. To ensure the effectiveness of these audits, the company meticulously identified operational sectors, procedures, and policies. However, FoodSafe Corporation did not utilize an organized audit timetable as part of its internal compliance audit process. While FoodSafe's Corporation organizational chart does not clearly indicate the audit team's position, the internal audit process is well-structured. Auditors familiarize themselves with established policies and procedures to gain a comprehensive understanding of their workflow. They engage in discussions with employees further to enhance their insights, ensuring no critical details are overlooked.

Subsequently, FoodSafe Corporation's auditors generate a comprehensive report of findings, serving as the foundation for necessary changes and improvements within the company. Auditors also follow up on action plans in response to nonconformities and improvement opportunities.

The company recently expanded its offerings by adding new products and services, which had an impact on its cybersecurity program. This required the cybersecurity team to adapt and ensure that these additions were integrated securely into their existing framework. FoodSafe Corporation commitment to enhancing its monitoring and measurement processes to ensure product quality and operational efficiency. In doing so, the company carefully considers its target audience and selects suitable methods for reporting monitoring and measurement results. This includes incorporating additional graphical elements and labeling of endpoints in their reports to provide a clearer and more intuitive representation of data, ultimately facilitating better decision-making within the organization.

Which change factors impacted FoodSafe's Corporation cybersecurity program? Refer to scenario 8.

- A. External changes
- B. Organizational changes
- C. Changes in technologies

Answer: B

NEW QUESTION # 82

.....

Thanks to modern technology, learning online gives people access to a wider range of knowledge, and people have got used to convenience of electronic equipment. As you can see, we are selling our NIS-2-Directive-Lead-Implementer learning guide in the international market, thus there are three different versions of our NIS-2-Directive-Lead-Implementer exam materials which are prepared to cater the different demands of various people. We here promise you that our NIS-2-Directive-Lead-Implementer Certification material is the best in the market, which can definitely exert positive effect on your study. Our PECB Certified NIS 2 Directive Lead Implementer learn tool create a kind of relaxing leaning atmosphere that improve the quality as well as the efficiency, on one hand provide conveniences, on the other hand offer great flexibility and mobility for our customers. That's the reason why you should choose us.

Reliable NIS-2-Directive-Lead-Implementer Test Guide: <https://www.examsreviews.com/NIS-2-Directive-Lead-Implementer-pass4sure-exam-review.html>

- NIS-2-Directive-Lead-Implementer PDF Dumps Files Download NIS-2-Directive-Lead-Implementer Free Dumps
- Associate NIS-2-Directive-Lead-Implementer Level Exam Open [www.exam4labs.com] and search for **【 NIS-2-**

