

High-quality Valid NIS-2-Directive-Lead-Implementer Exam Prep & Leading Provider in Qualification Exams & Authorized NIS-2-Directive-Lead-Implementer Reliable Test Syllabus



NIS 2 Directive Lead Implementer

LOCATION:
Live Online / Self Study

Date:
June 10-13, 2024
July 01-04, 2024 / July 22-25, 2024

COURSE TIMINGS:
9 am - 4 pm US CST Batch 1 For North America
10 am - 5 pm CET Batch 2 For EMEA

+1 (214) 447 6371 / +1 (469) 638 3677
+44 20 8144 4419 / +91 9 011 38 18 18

hello@smatica.com www.smatica.com

DOWNLOAD the newest Lead1Pass NIS-2-Directive-Lead-Implementer PDF dumps from Cloud Storage for free:
<https://drive.google.com/open?id=1Ds07eHswXa0kt6YPWU-1P4RB9gMvf0Ug>

Our PECB Certified NIS 2 Directive Lead Implementer exam question has been widely praised by all of our customers in many countries and our company has become the leader in this field. Our product boost varied functions and they include the self-learning and the self-assessment functions, the timing function and the function to stimulate the exam to make you learn efficiently and easily. There are many advantages of our NIS-2-Directive-Lead-Implementer Study Tool. If any questions or doubts exist, the client can contact our online customer service or send mails to contact us and we will solve them as quickly as we can. We always want to let the clients be satisfied and provide the best NIS-2-Directive-Lead-Implementer test torrent and won't waste their money and energy.

Lead1Pass is a professional website to specially provide training tools for IT certification exams and a good choice to help you pass NIS-2-Directive-Lead-Implementer exam, too. Lead1Pass provide exam materials about NIS-2-Directive-Lead-Implementer certification exam for you to consolidate learning opportunities. Lead1Pass will provide all the latest and accurate exam practice questions and answers for the staff to participate in NIS-2-Directive-Lead-Implementer Certification Exam.

>> Valid NIS-2-Directive-Lead-Implementer Exam Prep <<

Free PDF Quiz 2026 Newest PECB NIS-2-Directive-Lead-Implementer: Valid PECB Certified NIS 2 Directive Lead Implementer Exam Prep

Our NIS-2-Directive-Lead-Implementer exam questions are supposed to help you pass the exam smoothly. Don't worry about channels to the best NIS-2-Directive-Lead-Implementer study materials so many exam candidates admire our generosity of offering help for them. Up to now, no one has ever challenged our leading position of this area. The existence of our NIS-2-Directive-Lead-Implementer learning guide is regarded as in favor of your efficiency of passing the exam. And the pass rate of our NIS-2-Directive-Lead-Implementer training braindumps is high as 98% to 100%.

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

Topic	Details
Topic 1	<ul style="list-style-type: none"> • Fundamental concepts and definitions of NIS 2 Directive: This section of the exam measures the skills of Cybersecurity Professionals and IT Managers and covers the basic concepts and definitions related to the NIS 2 Directive. Candidates gain understanding of the directive's scope, objectives, key terms, and foundational requirements essential to lead implementation efforts effectively within organizations.
Topic 2	<ul style="list-style-type: none"> • Communication and awareness: This section covers skills of Communication Officers and Training Managers in developing and executing communication strategies and awareness programs. It emphasizes fostering cybersecurity awareness across the organization and effective internal and external communication during cybersecurity events or compliance activities.
Topic 3	<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 4	<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.

PECB Certified NIS 2 Directive Lead Implementer Sample Questions (Q57-Q62):

NEW QUESTION # 57

Which of the following entities are excluded from the scope of the NIS 2 Directive?

- A. Public administration entities involved in law enforcement activities
- B. Regulatory entities
- C. Entities with only marginal relevance to the areas of national security, public security, defense, or law enforcement activities

Answer: A

NEW QUESTION # 58

Scenario 5:Based in Altenberg, Germany, Astral Nexus Power is an innovative company founded by visionary engineers and scientists focused on pioneering technologies in the electric power sector. It focuses on the development of next-generation energy storage solutions powered by cutting-edge quantum materials. Recognizing the critical importance of securing its energy infrastructure, the company has adopted the NIS 2 Directive requirements. In addition, it continually cooperates with cybersecurity experts to fortify its digital systems, protect against cyber threats, and ensure the integrity of the power grid. By incorporating advanced security protocols, the company contributes to the overall resilience and stability of the European energy landscape. Dedicated to ensuring compliance with NIS 2 Directive requirements, the company initiated a comprehensive journey toward transformation, beginning with an in-depth comprehension of its structure and context, which paved the way for the clear designation of roles and responsibilities related to security, among others. The company has appointed a Chief Information Security Officer (CISO) who is responsible to set the strategic direction for cybersecurity and ensure the protection of information assets. The CISO reports directly to the Chief Executive Officer (CEO) of Astral Nexus Power which helps in making more informed decisions concerning risks, resources, and investments. To effectively carry the roles and responsibilities related to information security, the company established a cybersecurity team which includes the company's employees and an external cybersecurity consultant to guide them.

Astral Nexus Power is also focused on managing assets effectively. It consistently identifies and categorizes all of its digital assets, develops an inventory of all assets, and assesses the risks associated with each asset. Moreover, it monitors and maintains the assets and has a process for continual improvement in place. The company has also assigned its computer security incident response team (CSIRT) with the responsibility to monitor its on and off premises internet-facing assets, which help in managing organizational risks. Furthermore, the company initiates a thorough process of risk identification, analysis, evaluation, and treatment. By identifying operational scenarios, which are then detailed in terms of assets, threats, and vulnerabilities, the company ensures a comprehensive identification and understanding of potential risks. This understanding informs the selection and development of risk treatment strategies, which are then communicated and consulted upon with stakeholders. Astral Nexus Power's commitment is further

underscored by a meticulous recording and reporting of these measures, fostering transparency and accountability.

Has Astral Nexus Power followed all the necessary steps to manage assets in cyberspace in accordance with best practices? Refer to scenario 5.

- A. No, the company must also involve external third parties to review and validate its asset management processes
- **B. No, the company should also implement appropriate security controls after assessing the risks associated with each asset**
- C. Yes, the company has followed all the steps required to manage assets in cyberspace in accordance with best practices

Answer: B

NEW QUESTION # 59

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?

- **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

NEW QUESTION # 60

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.

According to scenario 2, MHospital is committed to issuing an official notification within four days of identifying an incident. Is this in compliance with the NIS 2 Directive requirements?

- A. No, the official notification should be issued within 48 hours of identifying the incident
- B. No, the official notification should be issued within 72 hours of identifying the incident
- **C. Yes, the official notification should be issued within 96 hours of identifying the incident**

Answer: C

NEW QUESTION # 61

Scenario 5:Based in Altenberg, Germany, Astral Nexus Power is an innovative company founded by visionary engineers and scientists focused on pioneering technologies in the electric power sector. It focuses on the development of next-generation energy storage solutions powered by cutting-edge quantum materials. Recognizing the critical importance of securing its energy infrastructure, the company has adopted the NIS 2 Directive requirements. In addition, it continually cooperates with cybersecurity experts to fortify its digital systems, protect against cyber threats, and ensure the integrity of the power grid. By incorporating advanced security protocols, the company contributes to the overall resilience and stability of the European energy landscape. Dedicated to ensuring compliance with NIS 2 Directive requirements, the company initiated a comprehensive journey toward transformation, beginning with an in-depth comprehension of its structure and context, which paved the way for the clear designation of roles and responsibilities related to security, among others. The company has appointed a Chief Information Security Officer (CISO) who is responsible to set the strategic direction for cybersecurity and ensure the protection of information assets. The CISO reports directly to the Chief Executive Officer (CEO) of Astral Nexus Power which helps in making more informed decisions concerning risks, resources, and investments. To effectively carry the roles and responsibilities related to information security, the company established a cybersecurity team which includes the company's employees and an external cybersecurity consultant to guide them.

Astral Nexus Power is also focused on managing assets effectively. It consistently identifies and categorizes all of its digital assets, develops an inventory of all assets, and assesses the risks associated with each asset. Moreover, it monitors and maintains the assets and has a process for continual improvement in place. The company has also assigned its computer security incident response team (CSIRT) with the responsibility to monitor its on and off premises internet-facing assets, which help in managing organizational risks. Furthermore, the company initiates a thorough process of risk identification, analysis, evaluation, and treatment. By identifying operational scenarios, which are then detailed in terms of assets, threats, and vulnerabilities, the company ensures a comprehensive identification and understanding of potential risks. This understanding informs the selection and development of risk treatment strategies, which are then communicated and consulted upon with stakeholders. Astral Nexus Power's commitment is further underscored by a meticulous recording and reporting of these measures, fostering transparency and accountability.

Based on scenario 5, Astral Nexus Power's hired an external consultant to provide guidance to the cybersecurity team compromised by the company's employees. Is this acceptable?

- **A. Yes, for establishing the cybersecurity team, decisions can be made to incorporate inside staff and guidance of an external expert**
- B. o, the cybersecurity team must be compromised by inside staff only to ensure confidentiality and avoid disclosing internal processes to external parties
- C. No, the cybersecurity team must be compromised by external cybersecurity experts only

Answer: A

NEW QUESTION # 62

.....

Our company is widely acclaimed in the industry, and our NIS-2-Directive-Lead-Implementer study materials have won the favor of many customers by virtue of their high quality. Started when the user needs to pass the qualification test, choose the NIS-2-Directive-Lead-Implementer study materials, they will not have any second or even third backup options, because they will be the

