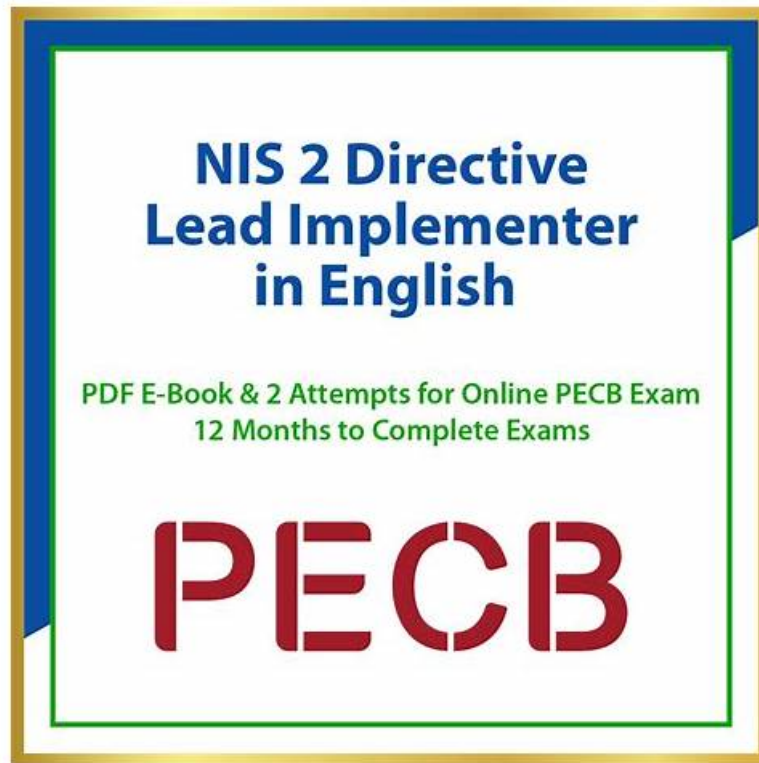


PECB - NIS-2-Directive-Lead-Implementer - PECB Certified NIS 2 Directive Lead Implementer High Hit-Rate Exam Success



What's more, part of that ExamDiscuss NIS-2-Directive-Lead-Implementer dumps now are free: <https://drive.google.com/open?id=1PmO9ILYV6Q-pqe56knrLZYp2pjqsDpZM>

The ExamDiscuss is one of the leading brands that have been helping PECB NIS-2-Directive-Lead-Implementer Certification aspirants for many years. Hundreds of PECB PECB Certified NIS 2 Directive Lead Implementer exam applicants have achieved the PECB Certified NIS 2 Directive Lead Implementer in Procurement and Supply PECB certification. All these successful PECB test candidates have prepared with real and updated PECB Certified NIS 2 Directive Lead Implementer in Procurement and Supply PECB Questions of ExamDiscuss. If you also want to become PECB Certified NIS 2 Directive Lead Implementer in Procurement and Supply PECB certified, you should also prepare with our PECB PECB Certified NIS 2 Directive Lead Implementer actual exam questions.

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

Topic	Details
Topic 1	<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.
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"> • 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 4	<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.

>> Exam NIS-2-Directive-Lead-Implementer Success <<

PECB NIS-2-Directive-Lead-Implementer Realistic Exam Success Pass Guaranteed Quiz

ExamDiscuss has one of the most comprehensive and top-notch PECB NIS-2-Directive-Lead-Implementer Exam Questions. We eliminated the filler and simplified the PECB Certified NIS 2 Directive Lead Implementer exam preparation process so you can ace the PECB certification exam on your first try. Our PECB NIS-2-Directive-Lead-Implementer Questions include real-world examples to help you learn the fundamentals of the subject not only for the PECB exam but also for your future job.

PECB Certified NIS 2 Directive Lead Implementer Sample Questions (Q61-Q66):

NEW QUESTION # 61

Which of the following EU regulations addresses illegal content, transparent advertising, and disinformation in digital space?

- A. Digital Markets Act
- B. Digital Operational Resilience Act
- C. Digital Services Act

Answer: C

NEW QUESTION # 62

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 the scenario above, answer the following question:

Is the role of the MHospital's CSIRT regarding vulnerability assessment in alignment with the requirements of Article 11 of the NIS 2 Directive?

- A. No, according to Article 11, the CSIRT should not conduct scanning of the network and information systems of the entity as this should be done during the coordinated vulnerability disclosure
- B. No, the CSIRT should not be involved in vulnerability management, as defined in Article 11
- **C. Yes, the role of the CSIRT is consistent with vulnerability assessment requirements specified in Article 11**

Answer: C

NEW QUESTION # 63

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

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

Answer: C

NEW QUESTION # 64

Which of the following teams continuously manages existing threats by establishing rules, identifying exceptions, and detecting emerging risks?

- A. Crisis management team
- **B. Security operations center team**
- C. Incident response team

Answer: B

NEW QUESTION # 65

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.

Based on the scenario above, answer the following question:

In which category SecureTech fit according to the NIS 2 Directive?

- A. Important entities
- **B. Essential entities**
- C. Critical entities

Answer: B

NEW QUESTION # 66

.....

We recommend you use PECB NIS-2-Directive-Lead-Implementer practice material to prepare for your NIS-2-Directive-Lead-Implementer certification exam. ExamDiscuss provides the most accurate and real PECB NIS-2-Directive-Lead-Implementer Exam Questions. These PECB NIS-2-Directive-Lead-Implementer practice test questions will assist you in better preparing for the final PECB NIS-2-Directive-Lead-Implementer exam.

NIS-2-Directive-Lead-Implementer Reliable Test Experience: <https://www.examdisscuss.com/PECB/exam/NIS-2-Directive-Lead-Implementer/>

- [illegible]

P.S. Free 2026 PECB NIS-2-Directive-Lead-Implementer dumps are available on Google Drive shared by ExamDiscuss:
<https://drive.google.com/open?id=1PmO9ILYV6Q-pqe56knrLZYp2piqsDpZM>