New NIS-2-Directive-Lead-Implementer Test Vce & Training NIS-2-Directive-Lead-Implementer For Exam

We will definitely not live up to the trust of users in our NIS-2-Directive-Lead-Implementer study materials. As you know, the users of our NIS-2-Directive-Lead-Implementer exam questions are all over the world. We have also been demanding ourselves with the highest international standards to support our NIS-2-Directive-Lead-Implementer training guide in every aspect. First of all, our system is very advanced and will not let your information leak out. It is totally safe to visit our website and buy our NIS-2-Directive-Lead-Implementer learning prep. You won't worry anything with our services.

It can be said that all the content of the NIS-2-Directive-Lead-Implementer study materials are from the experts in the field of masterpieces, and these are understandable and easy to remember, so users do not have to spend a lot of time to remember and learn. It takes only a little practice on a daily basis to get the desired results. Especially in the face of some difficult problems, the user does not need to worry too much, just learn the NIS-2-Directive-Lead-Implementer Study Materials provide questions and answers, you can simply pass the exam.

>> New NIS-2-Directive-Lead-Implementer Test Vce <<

Training PECB NIS-2-Directive-Lead-Implementer For Exam | New Soft NIS-2-Directive-Lead-Implementer Simulations

This NIS-2-Directive-Lead-Implementer exam prep material has been prepared under the expert surveillance of 90,000 highly experienced IT professionals worldwide. This updated and highly reliable Exams-boost product consists of 3 prep formats: PECB Certified NIS 2 Directive Lead Implementer (NIS-2-Directive-Lead-Implementer) dumps PDF, desktop practice exam software, and browser-based mock exam. Each format specializes in a specific study style and offers unique benefits, each of which is crucial to good PECB Certified NIS 2 Directive Lead Implementer (NIS-2-Directive-Lead-Implementer) exam preparation. The specs of each PECB NIS-2-Directive-Lead-Implementer exam questions format are listed below, you may select any of them as per your requirements.

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

Topic	Details
Topic 1	• 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	• 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 3	• 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 4	• 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 5	• 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.

PECB Certified NIS 2 Directive Lead Implementer Sample Questions (Q31-Q36):

NEW QUESTION # 31
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, the CISO reports directly to the CEO of Astral Nexus Power. Is this in alignment with best practices?

- A. No, this type of structure does not allow the CISO to properly exercise the mandate with regards to cybersecurity
- B. Yes, it is advisable for the CISO to report directly to the top management to facilitate the process of decision-making with respect to cybersecurity
- C. No, the current organizational structure impedes inter-departmental collaboration which would enable balanced distribution of tasks

Answer: B

NEW QUESTION # 32
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. Yes, the official notification should be issued within 96 hours of identifying the incident
- B. No, the official notification should be issued within 72 hours of identifying the incident
- C. No, the official notification should be issued within 48 hours of identifying the incident

Answer: A

NEW QUESTION # 33
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.
In terms of the NIST Framework, under which implementation tier does StellarTech fall based on the level of implementation of its risk management measures within the company? Refer to scenario 4.

- A. ITier 2: Risk informed
- B. Tier 3: Repeatable
- C. Tier 4: Adaptive

Answer: C

NEW QUESTION # 34
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.
Based on this scenario, answer the following question:
Which of the following screening levels did Solicure implement during the evaluation process for new employees?

- A. Level 2
- B. Level 3
- C. Level 4

Answer: C

NEW QUESTION # 35
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.
According to scenario 1, SecureTech strongly emphasizes adopting a proactive cybersecurity approach, primarily focusing on preventing cyber threats before they escalate into incidents that could result in substantial material or non-material damage. Is this in alignment with the NIS 2 Directive?

- A. No, this NIS 2 Directive focuses only on identifying and mitigating incidents rather than cyber threats
- B. Yes, the NIS 2 Directive prioritizes proactive cybersecurity to prevent cyber threats from causing significant harm or damage.
- C. No, the NIS 2 Directive strongly emphasizes adopting a reactive cybersecurity approach

Answer: B

NEW QUESTION # 36
......

Our PECB Certified NIS 2 Directive Lead Implementer (NIS-2-Directive-Lead-Implementer) exam questions are being offered in three easy-to-use and compatible formats. These PECB NIS-2-Directive-Lead-Implementer exam dumps formats offer a user-friendly interface and are compatible with all devices, operating systems, and browsers. The PECB Certified NIS 2 Directive Lead Implementer (NIS-2-Directive-Lead-Implementer) PDF questions file contains real and Valid NIS-2-Directive-Lead-Implementer Exam Questions that assist you in NIS-2-Directive-Lead-Implementer exam dumps preparation and boost the candidate's confidence to pass the challenging PECB Certified NIS 2 Directive Lead Implementer (NIS-2-Directive-Lead-Implementer) exam easily. The PECB Certified NIS 2 Directive Lead Implementer (NIS-2-Directive-Lead-Implementer) PDF dumps file work with all devices and operating system.