正確的-権威のあるNIS-2-Directive-Lead-Implementer試験参考書試験-試験の準備方法NIS-2-Directive-Lead-Implementer独学書籍

2026年JPTestKingの最新NIS-2-Directive-Lead-Implementer PDFダンプおよびNIS-2-Directive-Lead-Implementer試験エンジンの無料共有：https://drive.google.com/open?id=1q9kGbvCqnSik_O2vqSDShVfadbAmtq6L

JPTestKingは2008年に設立されましたが、現在、ハイパスNIS-2-Directive-Lead-Implementerガイドトレントマテリアルの評判が高いため、この分野で主導的な地位にあります。 NIS-2-Directive-Lead-Implementer試験問題には、長年にわたって多くの同級生が続いていますが、これを超えることはありません。過去10年以来、成熟した完全なNIS-2-Directive-Lead-Implementer学習ガイドR&Dシステム、顧客の情報安全システム、顧客サービスシステムを構築しています。有効なNIS-2-Directive-Lead-Implementer準備資料を購入したすべての受験者は、高品質のガイドトレント、情報の安全性、ゴールデンカスタマーサービスを利用できます。

PECB NIS-2-Directive-Lead-Implementer 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• 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.
トピック 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.
トピック 3	• 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.

>> NIS-2-Directive-Lead-Implementer試験参考書 <<

初段のNIS-2-Directive-Lead-Implementer試験参考書 | 最初の試行で簡単に勉強して試験に合格する & 最高のPECB PECB Certified NIS 2 Directive Lead Implementer

最近PECB試験はますます重要になっています。受験生たちはたいへん悩んでいるんでしょう。受験生としてのあなたを助けるために、我々は質量高いNIS-2-Directive-Lead-Implementer問題集を提供して、あなたは我々の商品を利用して、試験に合格することができます。我々の提供するNIS-2-Directive-Lead-Implementer問題集を信じてください。

PECB Certified NIS 2 Directive Lead Implementer 認定 NIS-2-Directive-Lead-Implementer 試験問題 (Q48-Q53):

質問 # 48
Scenario 7:CleanHydro is a forward-thinking company operating in the wastewater industry. Based in Stockholm, Sweden, the company is dedicated to revolutionizing wastewater treatment processes using advanced automated technology aiming to reduce environmental impact.
Recognizing the paramount importance of robust cybersecurity measures to protect its advanced technologies, CleanHydro is committed to ensuring compliance with the NIS 2 Directive. In line with this commitment, the company has initiated a comprehensive employee training program. To do so, the company adheres to Sweden's national cybersecurity strategy, which includes objectives, governance frameworks to guide strategy implementation and define roles and responsibilities at the national level, risk assessment mechanism, incident preparedness measures, a list of involved authorities and stakeholders, and coordination policies.
In addition, CleanHydro engaged GuardSecurity, an external cybersecurity consultancy firm, to evaluate and potentially improve the cybersecurity infrastructure of the company to ensure compliance with the NIS 2 Directive. GuardSecurity focused on strengthening the risk management process of the company.
The company started determining competence development needs by considering competence levels, comparing them with required competence levels, and then prioritizing actions to address competence gaps found based on risk-based thinking. Based on this determination, the company planned the competence development activities and defined the competence development program type and structure. To provide the training and awareness programs, the company contracted CyberSafe, a reputable training provider, to provide the necessary resources, such as relevant documentation or tools for effective training delivery. The company's top management convened a meeting to establish a comprehensive cybersecurity awareness training policy. It was decided that cybersecurity awareness training sessions would be conducted twice during the onboarding process for new employee to instill a culture of cybersecurity from the outset and following a cybersecurity incident.
In line with the NIS 2 compliance requirements, CleanHydro acknowledges the importance of engaging in communication with communities consisting of other essential and important entities. These communities are formed based on industry sectors, critical infrastructure sectors, or other relevant classifications. The company recognizes that this communication is vital for sharing and receiving crucial cybersecurity information that contributes to the overall security of wastewater management operations.
When developing its cybersecurity communication strategy and setting objectives, CleanHydto engaged with interested parties, including employees, suppliers, and service providers, to understand their concerns and gain insights. Additionally, the company identified potential stakeholders who has expressed interest in its activities, products, and services. These activities aimed to contribute to the achievement of the overall objectives of its cybersecurity communication strategy, ensuring that it effectively addressed the needs of all relevant parties.
According to scenario 7, how does CleanHydro align with the provisions of Article 29, Cybersecurity information-sharing arrangements, of the NIS 2 Directive?

- A. By engaging in communication with communities consisting of other essential and important entities regarding cybersecurity information
- B. By establishing a cybersecurity awareness training policy to build a cybersecurity culture
- C. By involving employees, suppliers, and service providers in the process of developing cybersecurity communication strategy and objectives

正解：A

質問 # 49
According to Article 10 of the NIS 2 Directive, what is one of the responsibilities of Member States concerning CSIRTs?

- A. Monitoring the request management and routingsystem of CSIRTs to ensure seamless and efficient transitions
- B. Informingthe Commission aboutthe identity of the CSIRT alongwith the CSIRT chosen as the coordinator
- C. Negotiatingdisclosuretimelines with CSIRTs and managingvulnerabilities that impact multiple entities

正解：B

質問 # 50
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.
Does Solicure effectively handle cyber crises, including all necessary steps? Refer to scenario 6.

- A. No, Solicure does not communicate with stakeholders during a cyber crisis, focusing only on technical measures
- B. No, Solicure primarily focuses on investigation and overlooks other crucial steps in handling a cyber crisis
- C. Yes, Solicure effectively follows all necessary steps

正解：C

質問 # 51
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 last paragraph of scenario 1, which of the following standards should SecureTech utilize to achieve its objectives concerning the protection of customers' data?

- A. ISO/IEC TR 27103
- B. ISO/IEC 27017
- C. ISO/IEC 27018

正解：C

質問 # 52
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 48 hours of identifying the incident
- C. No, the official notification should be issued within 72 hours of identifying the incident

正解：A

質問 # 53
.....

Directive-Lead-Implementer資格関連題 □ ▸ NIS-2-Directive-Lead-Implementer ◂を無料でダウンロード{ www.topexam.jp }ウェブサイトを入力するだけNIS-2-Directive-Lead-Implementer受験対策解説集

- NIS-2-Directive-Lead-Implementer資格講座 □ NIS-2-Directive-Lead-Implementer受験記 □ NIS-2-Directive-Lead-Implementer専門試験 □ 今すぐ ➡ www.goshiken.com □□□で▹ NIS-2-Directive-Lead-Implementer ◃を検索して、無料でダウンロードしてくださいNIS-2-Directive-Lead-Implementer資格取得講座
- 試験の準備方法-正確的なNIS-2-Directive-Lead-Implementer試験参考書試験-効率的なNIS-2-Directive-Lead-Implementer独学書籍 □ ➤ NIS-2-Directive-Lead-Implementer □を無料でダウンロード[www.mogiexam.com]ウェブサイトを入力するだけNIS-2-Directive-Lead-Implementer専門試験
- 試験の準備方法-便利なNIS-2-Directive-Lead-Implementer試験参考書試験-更新するNIS-2-Directive-Lead-Implementer独学書籍 □ 《 www.goshiken.com 》で➥ NIS-2-Directive-Lead-Implementer □を検索して、無料でダウンロードしてくださいNIS-2-Directive-Lead-Implementerコンポーネント
- NIS-2-Directive-Lead-Implementer試験参考書を検索して,PECB Certified NIS 2 Directive Lead Implementerの半分をパスします □ 時間限定無料で使える▹ NIS-2-Directive-Lead-Implementer ◃の試験問題は ➡ www.passtest.jp □□□サイトで検索NIS-2-Directive-Lead-Implementer技術内容
- NIS-2-Directive-Lead-Implementer受験練習参考書 □ NIS-2-Directive-Lead-Implementer試験復習 □ NIS-2-Directive-Lead-Implementer受験練習参考書 □ ▹ www.goshiken.com ◃を開き、✔ NIS-2-Directive-Lead-Implementer □✔□を入力して、無料でダウンロードしてくださいNIS-2-Directive-Lead-Implementer資格復習テキスト
- NIS-2-Directive-Lead-Implementer試験の準備方法｜正確的なNIS-2-Directive-Lead-Implementer試験参考書試験｜効果的なPECB Certified NIS 2 Directive Lead Implementer独学書籍 □ { www.goshiken.com }サイトにて□ NIS-2-Directive-Lead-Implementer □問題集を無料で使おうNIS-2-Directive-Lead-Implementer資格講座
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, whatoplay.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

さらに、JPTestKing NIS-2-Directive-Lead-Implementerダンプの一部が現在無料で提供されています：https://drive.google.com/open?id=1q9kGbvCqnSik_O2vqSDShVfadbAmtq6L