
**Exam : NIS 2 Directive Lead
Implementer**

**Title : PECB Certified NIS 2
Directive Lead Implementer**

Version : DEMO

1.Which of the following entities are included on the scope of the NIS 2 Directive?

- A. Diplomatic and consular missions of Member States in third countries
- B. Public administration entities whose activities are predominantly carried out in national security
- C. Entities engaged in nuclear power plant electricity production

Answer: C

Explanation:

The NIS 2 Directive includes entities operating in critical sectors, such as energy, including nuclear power plant electricity production, within its scope. These entities are classified as essential due to the potential high impact on societal and economic functions in the event of cybersecurity incidents.

2.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

Explanation:

The NIS 2 Directive requires entities to submit an official notification within 72 hours, followed by a final report within one month. However, an intermediate report can be submitted within 96 hours in certain conditions. MHospital's commitment to issuing an official notification within four days (96 hours) is compliant with this requirement, especially when interpreted as part of the broader phased reporting process.

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

C. Yes, the discovery phase is correctly defined

Answer: C

Explanation:

According to NIST SP 800-115, the discovery phase of penetration testing involves gathering information, defining objectives, and obtaining necessary approvals before conducting the actual testing. FoodSafe Corporation's approach - defining clear testing objectives and obtaining top management approval - correctly aligns with this definition.

4.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.

Which of the following crisis management planning approaches did Solicure adopt? Refer to scenario 6.

A. Resource-based approach

B. Crisis-driven approach

C. Resilience-based approach

Answer: B

Explanation:

Solicure prioritized the structuring of crisis response and developed a comprehensive exercise plan focused on improving decision-makers' ability to respond to cyber threats. This indicates a crisis-driven approach, which centers on preparing for and managing specific crisis scenarios to improve organizational responsiveness and minimize impact.

5.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, which risk level does the identified threat during StellarTech's assessment fall into?

A. Moderate

B. Low

C. Very low

Answer: C

Explanation:

The identified threat is described as theoretically possible but highly unlikely to materialize due to StellarTech's robust security measures, absence of prior incidents, and strong existing practices. These factors indicate that the likelihood and potential impact are minimal, placing the threat in the very low risk category.