NEBOSYSTEMS LTD

https://nebosystems.eu , mobile: +359 885 818 615 ,

e-mail: office@nebosystems.eu

Nebosystems is an IT solutions company founded in 2011. We specialize in building and maintaining both physical and virtual (private and public clouds) IT infrastructure. We provide services in the field of cybersecurity, DevOps, IT audit, server colocation, automation of activities related to system and network administration. We ensure technical compliance of IT infrastructure and information systems with industry standards, laws, European directives and regulations.

NIS2 Directive Compliance Checklist for Companies

In response to the evolving cybersecurity threats, the European Union has introduced the NIS2 Directive, setting a new standard for cybersecurity measures across member states. Understanding and complying with these requirements is crucial for organizations operating within the EU.

This checklist is designed to help companies understand whether they are affected by the NIS2 Directive (Directive (EU) 2022/2555) and need to comply with its cybersecurity requirements. Answering these questions will provide an initial assessment of your company's obligations under the Directive.

Section 1: Company Size and Type

1. **Is your company considered a medium-sized enterprise or larger according to the EU definition?** (More than 50 employees and an annual turnover or balance sheet exceeding €10 million)

   □ Yes

   □ No

2. **Does your company operate in the digital infrastructure, including as a DNS service provider, TLD name registry, or cloud computing service provider?**

   □ Yes

   □ No

3. **Is your company a small enterprise or microenterprise that plays a key role in society, the economy, or within specific sectors or types of service?** (Consider if your services are critical even if your company is small.)

   □ Yes

□ No

Section 2: Sector-Specific Questions

4. **Is your company involved in any of the following sectors?**

   □ Energy

   □ Transport

   □ Banking

   □ Financial Market Infrastructure

   □ Health sector

   □ Drinking water

   □ Digital infrastructure

   □ Public administration

   □ Space

   □ None of the above

5. **Does your company provide essential services within these sectors that, if disrupted, would have a significant impact on societal or economic activities?**

   □ Yes

   □ No

Section 3: Operational Impact

6. **Does your company rely heavily on network and information systems for the provision of your services?**

   □ Yes

   □ No

7. **In the event of a cybersecurity incident, could your company's services be significantly disrupted, leading to substantial financial loss or societal impact?**

   □ Yes

   □ No

Section 4: Exclusions

8. **Is your company's primary activity related to national security, public security, defense, or law enforcement?** (Note: If only marginally related, you might still fall under the Directive.)

   □ Yes

   □ No

9. **Is your company a public administration entity that predominantly carries out activities in the areas of national security, public security, defense, or law enforcement?**

   □ Yes

   □ No

Section 5: Additional Considerations

10. **Has your company been previously identified as an operator of essential services under the NIS Directive or any national legislation related to cybersecurity?**

    □ Yes

    □ No

11. **Is your company part of the supply chain for critical services in any of the sectors identified in question 4?**

    □ Yes

    □ No

Conclusion

- **Questions 1, 2, or 3 (Company Size and Type):** If you answered **"Yes"** to any of these, your company falls within the scope of the NIS2 Directive due to its size, operation within digital infrastructure, or significant role despite being a small or microenterprise. **Next Steps:** Assess specific obligations under the NIS2 Directive and begin implementing necessary cybersecurity measures and reporting mechanisms.

- **Question 4 (Sector Involvement):** A **"Yes"** response indicates your company operates in a sector directly affected by the NIS2 Directive. **Next Steps:** Identify sector-specific cybersecurity requirements and engage with sector regulators or national cybersecurity authorities for guidance.

- **Question 5 (Provision of Essential Services):** If **"Yes,"** your services are crucial, making compliance with the NIS2 Directive imperative to ensure service continuity and security. **Next Steps:** Prioritize establishing a comprehensive risk management framework and incident response plan as per NIS2 requirements.

- **Questions 6 and 7 (Operational Impact):** Affirmative answers highlight your reliance on network and information systems and potential significant impacts from cybersecurity incidents. **Next Steps:** Strengthen your cybersecurity infrastructure, focusing on resilience and rapid incident response capabilities.

- **Questions 8 and 9 (Exclusions):** If you answered **"Yes,"** your company might be excluded due to its primary focus on national security or law enforcement. However, marginal involvement doesn't grant exclusion. **Next Steps:** Clarify your exclusion status with legal experts and, if applicable, review your cybersecurity practices to ensure they're adequate for your operational needs.

- **Question 10 (Previous Identification as Essential Service Operator):** A **"Yes"** answer suggests your company was already under obligations similar to those in the NIS2 Directive, which will likely continue or expand under the new directive. **Next Steps:** Update your cybersecurity and compliance strategies to align with NIS2 enhancements and consult with authorities for transitional requirements.

- **Question 11 (Part of the Supply Chain for Critical Services):** Answering **"Yes"** indicates your role in the supply chain could bring you under the NIS2 Directive's purview, especially with its increased focus on supply chain security. **Next Steps:** Evaluate your cybersecurity practices in the context of supply chain integrity, collaborate with your partners to understand your shared responsibilities, and implement any necessary security and reporting enhancements.

Please note that this checklist provides a preliminary assessment, and the specific obligations under the NIS2 Directive may vary based on national transposition and interpretation by regulatory authorities.

General Advice

Regardless of your answers, it's advisable for all companies, especially those operating within or closely related to critical sectors, to adopt robust cybersecurity measures. The evolving cybersecurity landscape and the interconnected nature of digital services mean that comprehensive security practices are essential for resilience against cyber threats.

For companies potentially falling under the NIS2 Directive, consider the following steps:

1. **Review and Update Security Policies:** Ensure that your cybersecurity policies are up-to-date and align with the best practices.

2. **Engage with Regulatory Authorities:** Reach out to your national cybersecurity authority or sector-specific regulatory bodies to clarify your status under the NIS2 Directive and to obtain guidance on compliance.

3. **Consult Legal and Cybersecurity Experts:** Seek advice from professionals specializing in cybersecurity law and technical security measures to ensure that your company meets all legal obligations and effectively mitigates cyber risks.

4. **Implement a Compliance Plan:** Develop or update your cybersecurity compliance plan to address the requirements of the NIS2 Directive, focusing on risk management, incident reporting, supply chain security, and other relevant areas.

Remember, even if your company is not directly affected by the NIS2 Directive, adopting its principles can enhance your cybersecurity posture and potentially offer a competitive advantage by demonstrating a commitment to security to your clients and partners.

Ready to ensure your company is NIS2 compliant? Contact Nebosystems today for expert NIS2 compliance consulting. Our team is dedicated to helping you navigate these regulations, ensuring your cybersecurity measures are robust and compliant.

Partnering with Nebosystems for Comprehensive NIS2 Compliance

Navigating the complexities of NIS2 compliance demands not only an in-depth understanding of the requirements but also access to advanced cybersecurity solutions. Nebosystems offers a holistic approach to cybersecurity, providing a suite of solutions and services designed to meet and exceed the NIS2 compliance standards. By partnering with Nebosystems, organizations can ensure that their IT infrastructure is robustly protected against current and future cyber threats, aligning with the European Union’s vision for a secure and resilient digital future.

Implementing Robust Cybersecurity Measures

In alignment with the NIS2 Directive’s mandates, organizations are required to adopt a holistic approach to cybersecurity, implementing a blend of technical and organizational measures designed to safeguard networks and information systems. Nebosystems offers a comprehensive suite of solutions tailored to meet these rigorous standards, ensuring robust protection across all facets of IT infrastructure.

Comprehensive IT Infrastructure Protection

To secure the IT infrastructure against a broad spectrum of cyber threats, the NIS2 Directive prescribes several critical protective measures. Nebosystems’ advanced solutions are at the forefront of addressing these requirements:

- **Network Segregation:** Leveraging cutting-edge technologies like Hillstone Networks Next-Generation Firewalls (NGFW), Nebosystems can ensure effective network segmentation, crucial for isolating sensitive data and minimizing the impact of potential breaches. Our solutions provide a fortified barrier, separating critical assets from less secure areas of the network.

- **Traffic Filtering:** Our NGFW solutions play a pivotal role in scrutinizing and managing both inbound and outbound network traffic. By enforcing stringent filtering rules, we prevent unauthorized access and effectively block malicious traffic, safeguarding the integrity of your network.

- **Administrative Environment Security:** Protecting the administrative environment is paramount to maintaining system integrity. Nebosystems utilizes Hillstone Networks NGFW to secure these critical areas, preventing unauthorized access and potential system configuration breaches.

- **Unauthorized Device Usage Prevention:** With the proliferation of devices accessing corporate networks, controlling the transfer of sensitive information is vital. Nebosystems can employ advanced Data Loss Prevention (DLP) technologies from industry leaders like Fortra and Trellix, effectively preventing data leaks and unauthorized device usage.

- **Data Encryption:** Nebosystems advocates for robust data protection measures, implementing full-disk encryption solutions such as Bitdefender Full-disk Encryption to ensure that even in the event of unauthorized access, data remains secure and indecipherable.

· **Information and Communication Systems Management:** The secure and efficient administration of information and communication systems is critical. Nebosystems harnesses the power of Netwrix Privileged Access Management (PAM) to ensure that only authorized personnel have access to critical systems, significantly reducing the risk of insider threats.

· **Access Control:** Our comprehensive PAM solutions extend to thorough access management, enforcing the principle of least privilege and ensuring that individuals have only the necessary access to perform their duties, thereby enhancing overall security.

· **Remote Access Security:** In today's remote work era, securing remote access points is imperative. Nebosystems can integrate solutions like Hillstone NGFW and N-Able Take Control with Netwrix PAM to create a secure environment for remote operations, ensuring seamless productivity without compromising security.

· **Software and Firmware Protection:** Keeping software and firmware up-to-date is crucial for maintaining system security. Nebosystems' implementation of Bitdefender Patch Management ensures that all software and firmware components are regularly updated, closing vulnerabilities and fortifying defenses.

· **Malware Protection:** Nebosystems adopts a multi-layered approach to malware protection, deploying comprehensive solutions from Trellix and Bitdefender, among others, to provide robust defense against a wide array of malware threats, ensuring the integrity and availability of your digital assets.

· **Web Server Security:** As the gateway to your online services, web servers require stringent protection. Nebosystems leverages Radware WAF and DDoS protection solutions to secure web servers against attacks and service disruptions, maintaining the continuity and reliability of your online presence.

· **DNS Security:** The integrity and availability of the Domain Name System (DNS) are fundamental to the functionality of internet-based services.

· **Continuous Monitoring:** Nebosystems emphasizes the importance of continuous monitoring, employing advanced systems to detect potential security incidents at an early stage, enabling proactive response and mitigation.

· **Automated Incident Management:** The implementation of Security Information and Event Management (SIEM) systems, such as those provided by Trellix and SecureVisio, automates the detection, analysis, and response to security incidents, enhancing the organization's capability to swiftly address threats and maintain compliance with NIS2 reporting obligations.

Protecting Public Information Systems and Services

For public-facing information systems and services, Nebosystems implements essential measures to ensure compliance with NIS2 requirements and safeguard these critical assets:

· **Multi-Factor Authentication (MFA):** Nebosystems advocates for the implementation of MFA, adding an extra layer of security to system and data access, ensuring that authentication requires multiple pieces of evidence, thus significantly reducing the risk of unauthorized access.

· **Web Application Firewall (WAF) Protection:** To defend web applications against attacks, Nebosystems can employ robust WAF solutions, such as AppWall by Radware, providing comprehensive protection by monitoring and filtering HTTP traffic, thereby safeguarding your web applications from potential threats.

· **DDoS Protection:** Distributed Denial-of-Service (DDoS) attacks can cripple online services. Nebosystems utilizes Radware’s DDoS Protection Solutions to ensure the availability and reliability of online services, protecting against service disruptions caused by DDoS attacks.

· **Regular Penetration Testing:** Nebosystems could conduct penetration tests to proactively identify and address vulnerabilities within public-facing systems and services, enabling organizations to remediate potential weaknesses before they can be exploited by attackers.

Ready to ensure your company is NIS2 compliant? Contact Nebosystems today for expert NIS2, DORA and GDPR compliance consulting. Our team is dedicated to helping you navigate these regulations, ensuring your cybersecurity measures are robust and compliant.