Your NIS2 Compliance Checklist: 09 Steps to Prepare

The NIS2 Directive from the EU brings new requirements for businesses to boost cybersecurity, conduct regular audits, and quickly report incidents. These rules are mandatory for organisations offering essential services, but they're also important for anyone wanting to work with those organisations.

Here's how to get your business ready for NIS2 compliance:

01 Build a Cybersecurity Policy

Action: Create a clear cybersecurity policy that outlines how you manage risks, protect data, and respond to incidents.

Why this matters: NIS2 requires businesses to have a solid cybersecurity strategy. Your policy is your roadmap for keeping data and systems secure.

02 Regularly Assess Cyber Risks

Action: Conduct regular risk assessments to identify potential threats and vulnerabilities in your systems.

Why this matters: Risk management is central to NIS2. Understanding where your weaknesses are will help you take steps to fix them.

03 Secure Your Supply Chain

Action: Review the cybersecurity practices of your suppliers and partners. Ensure they meet your security standards.

Why this matters: NIS2 places responsibility on businesses to ensure their supply chains are secure. Any weak links can expose you to risk.

04 Set Up Incident Detection and Response

Action: Put systems in place to detect cyber threats early and respond quickly if an attack happens.

Why this matters: Being prepared to handle incidents is crucial. NIS2 requires swift reporting, so having an effective response system is essential.

05 Report Incidents on Time

Action: Establish a clear process for reporting significant cybersecurity incidents to the relevant authorities within the required timeframe.

Why this matters: NIS2 sets specific deadlines for reporting incidents. Missing these deadlines could result in penalties.

06 Ensure Business Continuity Plans

Action: Develop and test a business continuity plan that ensures you can keep operating during a cyberattack or IT failure.

Why this matters: Cyber incidents can disrupt your business. A strong continuity plan will help you recover faster and limit the damage.

07 Train Your Employees on Security

Action: Provide regular security training for all staff to help them understand the risks and follow best practices.

Why this matters: Human error is often the weakest link in cybersecurity. Training employees is an effective way to prevent breaches.

08 Work with Authorities and Partners

Action: Create a clear cybersecurity policy that outlines how you manage risks, protect data, and respond to incidents.

Why this matters: NIS2 encourages cooperation to strengthen collective cybersecurity efforts. Sharing knowledge can help prevent attacks.

09 Appoint a Compliance Lead

Action: Designate a person or team responsible for overseeing NIS2 compliance and managing your cybersecurity practices.

Why this matters: Having someone in charge of compliance ensures that your organisation stays on track with NIS2 requirements.

How Certes DPRM Can Help Your Business?

Certes DPRM solution can help organisations meet NIS2 compliance by focusing on protecting data itself, rather than just the surrounding infrastructure. With features like data segmentation and encryption, Certes ensures that even if a breach occurs, the data remains unusable to attackers. This proactive approach aligns with NIS2's focus on cybersecurity, helping mitigate risks like ransomware and ensuring compliance without requiring major infrastructure changes.

Ready to Get NIS2 Compliant?

Contact our team today to learn how Certes DPRM can help your business become NIS2 compliant and secure your critical data.