Resources

NIS 2 CHECKLIST

As a business considers what needs to be done to comply with the NIS2 Directive, here's a high-level checklist that is helpful for perusal.

1. Understand Applicability:

Determine if your organization falls under the essential or important entities as outlined in Annexes I and II, considering your size, sector, and activities within the EU.

2. Risk Management Measures:

Implement appropriate technical, operational, and organizational measures to manage risks to network and information systems security, considering state of the art, cost, size, risk likelihood, and severity.

3. Incident Response Plan

Develop an incident handling and response plan, including detection, analysis, containment, eradication, recovery, and post-incident activities.

4. Business Continuity Planning:

Ensure plans for business continuity, backup management, and disaster recovery are in place and tested regularly.

5. Supply Chain Security:

Assess and manage the cybersecurity risks of direct suppliers and service providers, considering their security practices and the impact on your supply chain.

6. Security of Acquisitions:

Ensure security in the acquisition, development, and maintenance of your network and information systems, including handling vulnerabilities and employing secure development practices.

7. Training and Awareness:

Conduct regular cybersecurity training and promote cyber hygiene practices among all employees, including management.

Resources

NIS 2 CHECKLIST

8. Incident Reporting:

Report significant incidents to the relevant CSIRT or competent authority within the specified timelines, and follow the multi-stage reporting approach as required.

9. Designate a Representative:

If not based in the EU but offering services within it, designate an EU representative in one of the member states where services are offered.

10. Information Sharing:

Engage in information sharing about vulnerabilities, incidents, and threats with relevant authorities and possibly with other entities, as appropriate.

11. Compliance with Additional Requirements

For ENISA-registered entities, comply with any additional cybersecurity requirements and guidance specified by the Commission.

12. Review and Update Security Policies:

Regularly review and update security policies and measures to adapt to new threats and comply with evolving NIS2 requirements.

13. Board Approval and Oversight:

Ensure the organization's management body approves the cybersecurity risk management measures and oversees their implementation.

14. Prepare for Audits and Inspections:

Be ready for regular and targeted security audits, inspections, and scans by competent authorities, and cooperate with them as required.

15. Legal and Regulatory Updates:

Stay informed about national implementations of NIS2 and any sector-specific EU legal acts that may affect compliance obligations.