NIS2
IMPLEMENTATION SUPPORT

Network and Information Systems Directive

Protect your business and sensitive data against cyber threats and enhance your organization's cybersecurity by compliance with NIS2

To comply with the NIS2 directive, organizations must consider implementing the following services:

- **Risk management** - To comply with the new Directive, organizations must take measures to minimize cyber risks. These measures include incident management, stronger supply chain security, enhanced network security, better access control, and encryption.
- **Corporate accountability** - NIS2 requires corporate management to oversee, approve, and be trained on the entity's cybersecurity measures and to address cyber risks. Breaches may result in penalties for management, including liability and a potential temporary ban from management roles.
- **Reporting obligations** - Essential and important entities must have processes in place for prompt reporting of security incidents with significant impact on their service provision or recipients. NIS2 sets specific notification deadlines, such as a 24-hour "early warning".
- **Business continuity** - Organizations must plan for how they intend to ensure business continuity in the case of major cyber incidents. This plan should include considerations about system recovery, emergency procedures, and setting up a crisis response team.

The scope of our NIS2 implementation support services

Audit services

- NIS2 compliance check
- Assessment of internal processes and procedures
- Identifying gaps and helping in becoming NIS2 compliant

Threat detection and monitoring

- Configuration of security detection and monitoring tools (Microsoft Defender stack and Microsoft Sentinel)
- 24/7 or 8/5 security threats monitoring

Risk management

- Risk identification, analysis and assessment
- Risk Treatment
- Risk monitoring and reporting
- Services based on Microsoft Defender XDR, Purview Compliance Manager and Insider Risk

Incident response and reporting

- 24/7 SOC service to identify and resolve incidents
- Triage identified incidents (Microsoft Sentinel)
- Performing defensive actions: containment, eradication and recovery
- Report incidents to respective authorities

Cybersecurity Education and Awareness

- Preparation of training materials
- Delivery of cybersecurity trainings
- Coordination of phishing and awareness campaigns (O365 Phishing Simulation and Learning Paths)

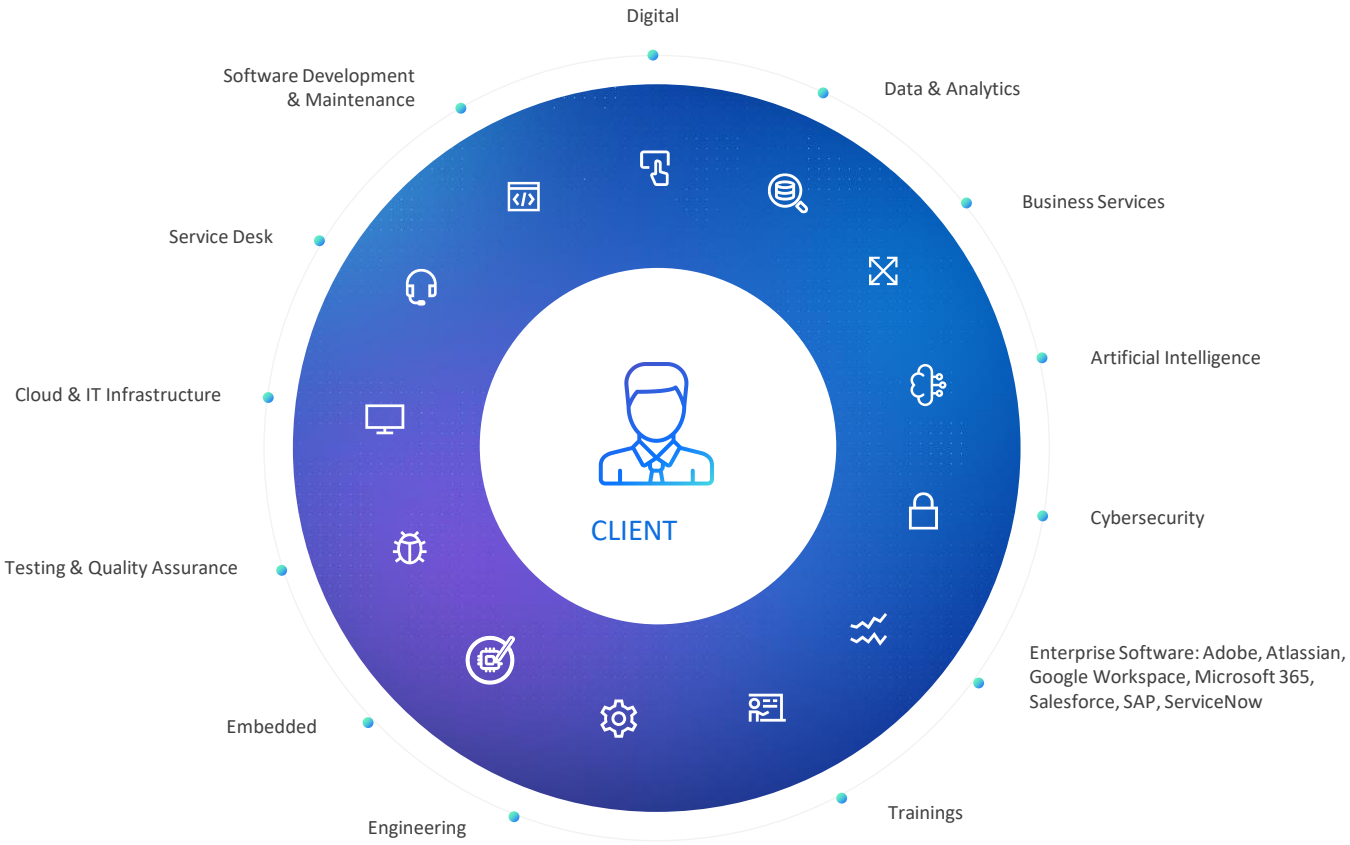
BCP planning

- Critical business activities identification
- Business continuity risk assessment
- Business continuity plan development:
- Plan approval and implementation
- Ongoing monitoring

Why become NIS2 compliant with SII:

- Highly qualified consultants to help strengthen your organization security environment
- Better response to cyber threats
- Significantly reduced successful attack risk
- Compliance with regulatory requirements,
- Better protection against regulatory fines
- Services based on crucial Microsoft products (Defender, Purview, etc.)

Offer – One-stop shop



Tangible Benefits / Desired Outcomes

- ✓ You take care of your business development - we take care of the cloud
- ✓ Our architects will support you in the latest technologies
- ✓ We are ready to maintain your infrastructure with dedicated support team

Microsoft Solutions Partner
Microsoft Cloud

Why Sii

600 certifed experts

Solution Architects, Network Engineers, Security Engineers, DevOps Architects, Data Engineers, Azure Administrators, Azure Developer, Cybersecurity Artchitects, D365 Consultants, Power BI Analysts

Leading cloud services

Microsoft Azure, Microsoft 365, Dynamics 365, Power Platform

Innovative industry solutions

For manufacturing banking, healthcare, real estate and public sectors

End-to-end Project Support

Mrom preliminary data analysis, target model creation, implementation on dedicated devices to maintenance