DORA IMPLEMENTATION SUPPORT

Digital Operational Resilience Act

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

To comply with the DORA act, organizations must consider implementing the following services:

- **ICT Risk Management** - To comply with the new Directive, organizations must take measures to minimize cyber risks. These measures include establishing processes to monitor, log, and classify ICT-related incidents, reporting incidents to relevant regulators and publishing reports for ICT-related incidents to clients and users
- **Digital Operational Resilience Testing** – DORA requires company to regularly test the operational resilience of digital systems and processes
- **Managing ICT Third-Party Risk** – organizations must manage risks associated with third-party providers and implement robust governance policies and procedures
- **ICT incidents reporting and Information-Sharing** – company needs to collaborate with other financial entities and regulators to share threat intelligence and incident details

The scope of our DORA implementation support services

Audit services

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

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

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

Cybersecurity Education and Awareness

- Preparation of training materials
- Delivery of cybersecurity trainings
- Coordination of phishing and awareness campaigns

Risk management

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

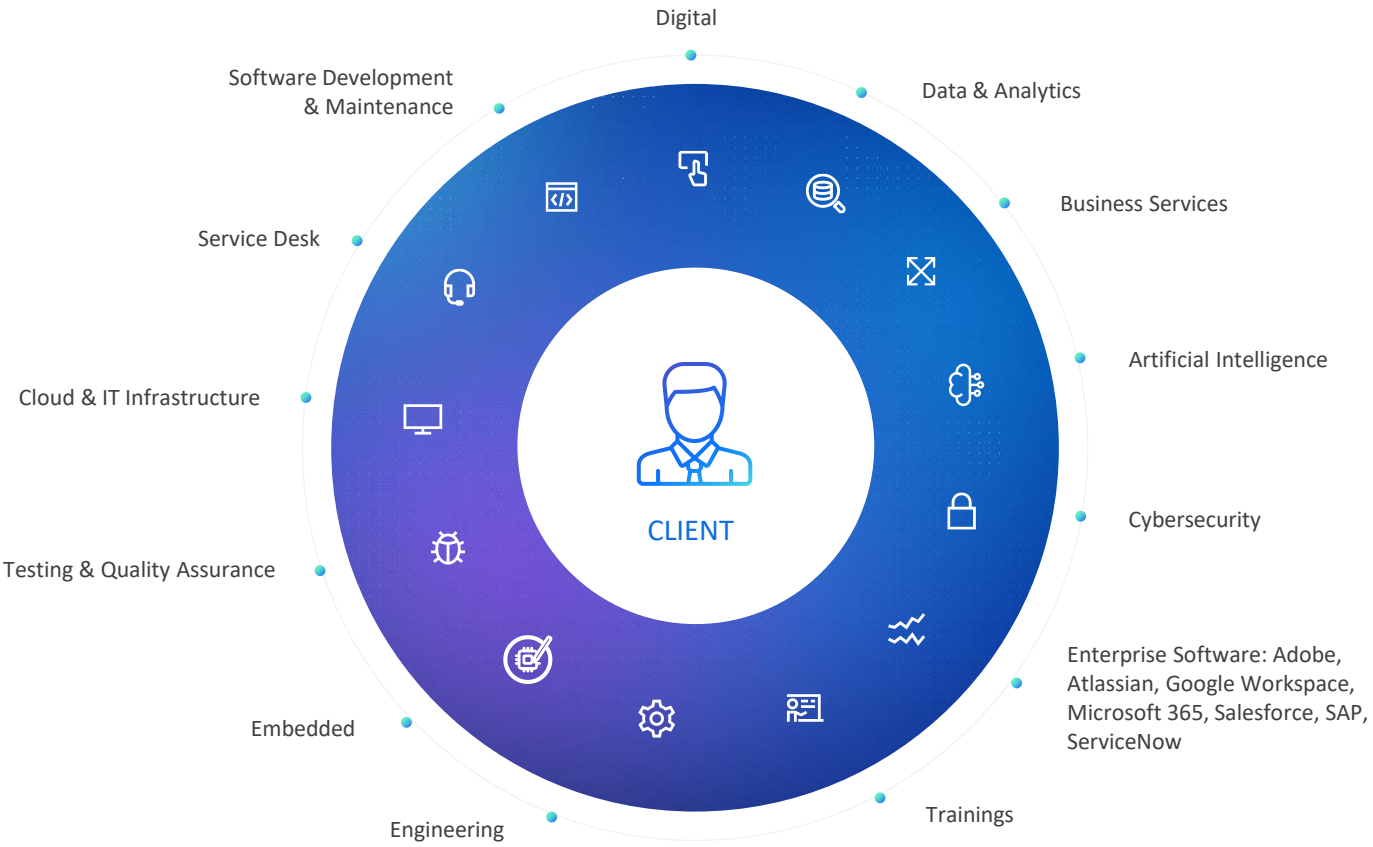
BCP planning

- Critical business activities identification
- Business continuity risk assessment
- Ongoing monitoring

Why become DORA compliant with SII:

- Highly qualified consultants to help strengthen your organization security environment
- Better understanding of DORA legislation
- Assistance with regulatory assessment of existing documentation and organizational maturity against DORA's requirements
- Help in preparation of the DORA roadmap and in it's practical adaptation
- Compliance with regulatory requirements
- Better protection against regulatory fines
- Services based on crucial Microsoft products (Defender, Sentinel, etc.)
- Significantly reduced successful attack risk

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