NIS2, CER and DORA

A briefing for executives

Blue River Experts

Member of the Art of Innovation Network

Early 2023 was a significant milestone in the security posture of the European Union. Two directives and one regulation were launched, pointing out the significance of cyber security within the EU.

The **Network and Information Security Directive 2** (NIS2) mandates member states to implement measures for enhancing the cyber security of network and information systems. Key objectives include establishing national incident notification systems and fostering cooperation among EU member states and institutions within the realm of cyber security. Furthermore, NIS2 extends its scope to include critical service operators including digital service providers. These entities are required to implement security measures that are appropriate and proportionate to their operations and they must promptly report significant cyber security incidents to the national regulatory body.

The **Critical Entities Resilience Directive** (CER) focuses on protecting critical infrastructure. While NIS2 has a focus on Cyber Security, CER addresses all aspects of resilience of critical entities. CER is aligned with NIS2 and also has substantially increased the scope of applicability.

Both NIS2 and CER need to be transposed into national law by 2024.

The **Digital Operations Resilience Act** (DORA) addresses a significant concern within EU financial regulations. Prior to DORA, financial institutions primarily dealt with major operational risk categories by allocating capital, but they did not comprehensively manage all facets of operational resilience. DORA introduces a comprehensive approach that applies to a wide spectrum of financial entities, including credit institutions, electronic money institutions, investment firms, insurance undertakings, and re-insurance undertakings.

NIS, CER, and DORA each address different aspects of security, however, they are closely aligned and there are some common themes including:

- Increased emphasis on the importance of identifying and mitigating risks
- Enhanced information sharing of threat intelligence and coordination between entities
- The impact of the supply chain on the security posture of entities
- Verification of the resilience of providers of essential services

Above mentioned directives and regulation affect nearly all organizations despite their official scope and executives should be aware of their objectives, concepts, legal and regulatory frameworks and the resulting obligations of organizations

Our briefing will give you a comprehensive overview, will help you to understand if your organization is affected and explain key steps and deadlines to achieve compliance in the most effective way.

Outline

Introduction

- Introduction of NIS2, CER, and DORA
- Similarities and differences
- The importance for your organization

Requirements and Compliance

- Overview and objectives
- Key terms and concepts
- Legal and regulatory framework
- Which organizations are affected and to what extent
- What are the obligations of affected organizations
- Roles and responsibilities of executives in ensuring compliance
- The potential impact of non-compliance and associated penalties

Implementation & Timeline

- Key Implementation Steps
- Deadlines
- Challenges and potential risks

Q&A

Duration

- 60 minutes presentation
- 30 minutes Q&A