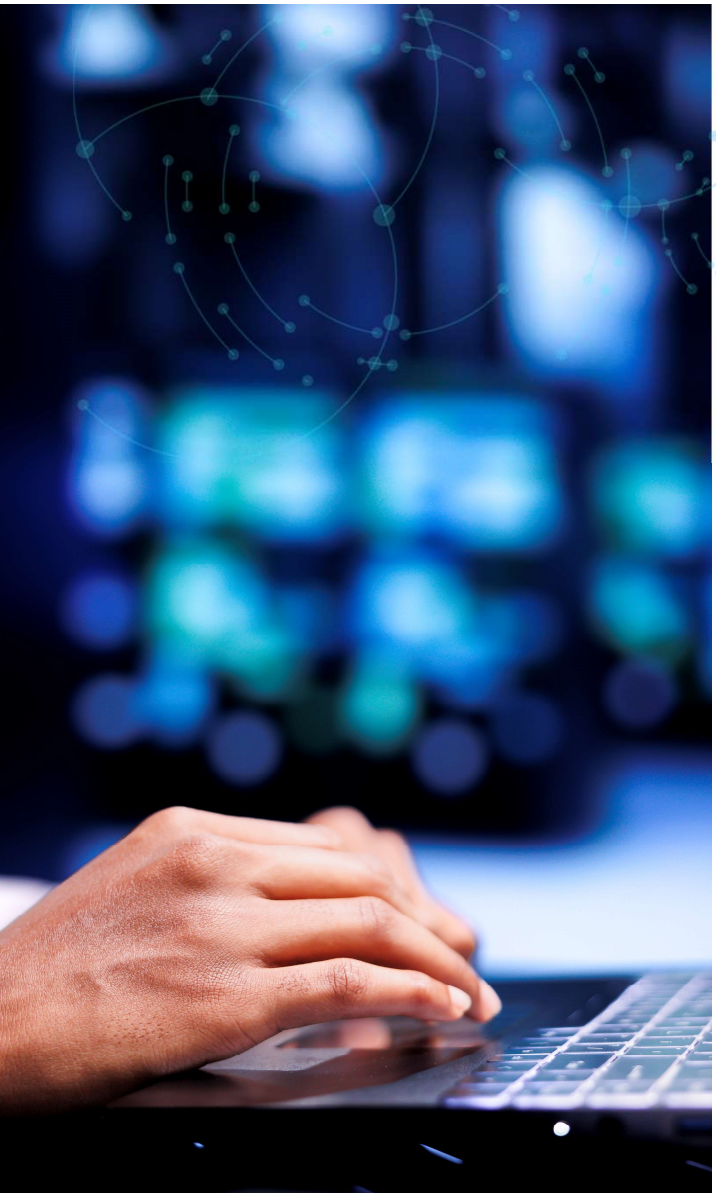
NIS 2

The (Regulatory) Cyber Challenge

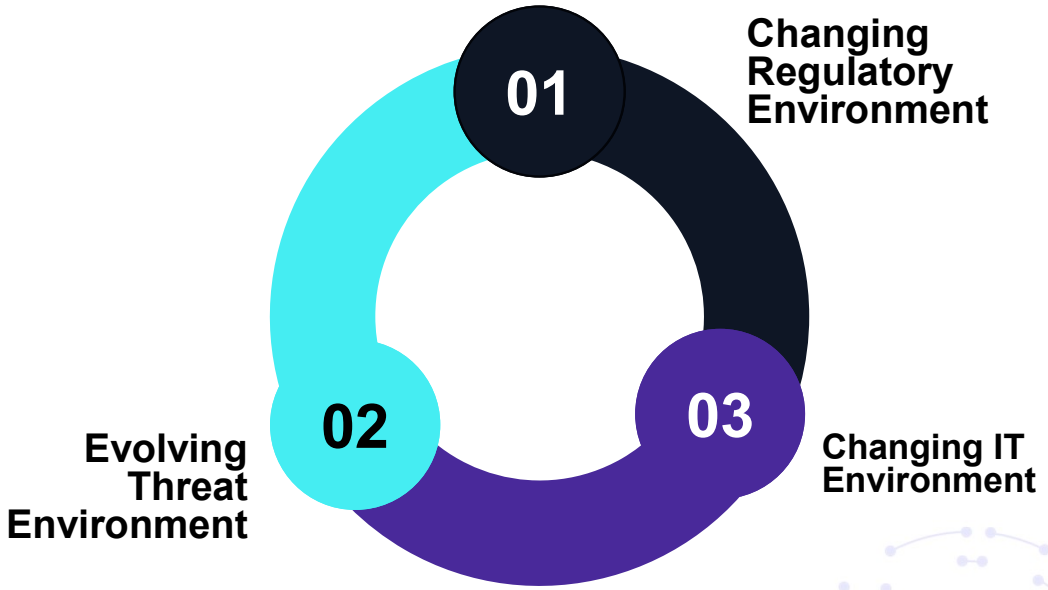
Introduction

Uwe Wirtz
Freelancer & CISO



The never-ending perfect storm

Cyberspace is now regarded as the backbone of digital society and economic growth. However, cyber security incidents are increasing and may disrupt the supply of essential services, and undermine trust in digital services and products.



Network & Information Security Directive 2 (NIS 2)

Entry into force:

NIS 2 was finalized and accepted in December of 2022 and will be fully applicable beginning in October of 2024.

EU member states have until October 2024 to transpose the contents of this directive into local law and make sure it enters effect by October 2024.

Requirements stated in the NIS 2 directive serve as a **minimum baseline**, allowing member states to introduce stricter requirements.

2022

1

Q4/2022

NIS 2 accepted and published EU-wide

2023-24

2

Until 10/2024

Member states must transpose requirements into local law

2024

3

From 10/2024

Entry into force in every member state

Essential Content*

Incident Handling

Stricter notification requirements and additional bodies of oversight

Risk Management

Requirements for formal Risk Management procedures and related policies

Human Resources Security

Cybersecurity awareness, identity and access as well as asset management

Security in networks & information systems

Security to be considered in development, acquisition, maintenance of information systems and networks

Business Continuity Management

Business Continuity, Backup and crisis management requirements

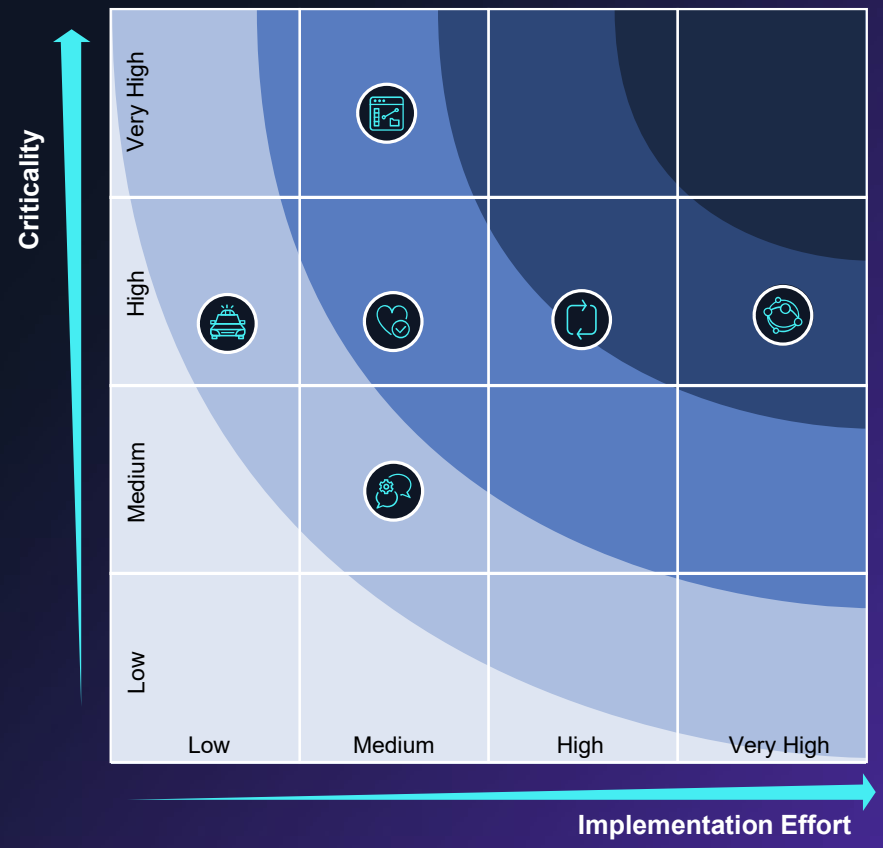
Information Sharing

Cybersecurity-related information is to be shared with bodies of oversight across the EU

*Extract of most relevant requirement clusters.

The aim of NIS 2 is to establish EU-wide harmonized requirements to ensure resilience against cyber-attacks and improve responses to multi-national incidents.

NIS 2 Impact Heatmap



NIS 2 Requirements in detail

Req.	What is key?
	Establishing Incident Handling
	Implementing Security in networks & information systems
	Increasing Human Resources Security, Access and Asset Management
	Aligning Risk Management processes with business objectives
	Implementing Business Continuity Management and practicing Backup and Crisis management
	Identifying and collaborating with bodies of oversight – Information sharing

Key Take Aways

Take Away 1

Don’t wait, start NOW!

Take Away 2

- Customer Requirements
- Gap Assessment for Technology & Processes.
- Involve Management
- Internal & External Auditors
- Focus on Risk Management

Take Away 3

- Budget Estimation, Funding & Project Ramp-up
- Build-up Internal Skills / External Partners

Take Away 4

Integrate Cybersecurity into the DNA of your Company

Thank you