NIS2: Achieving fit-for-purpose cyber risk integration

The EU's Directive for Network and Information Systems (NIS2) has been transposed into national law by most EU member states. It requires a broad range of sectors to upgrade their approaches to cyber security subject to reporting requirements and liability for on-compliance down to individual executive board members.

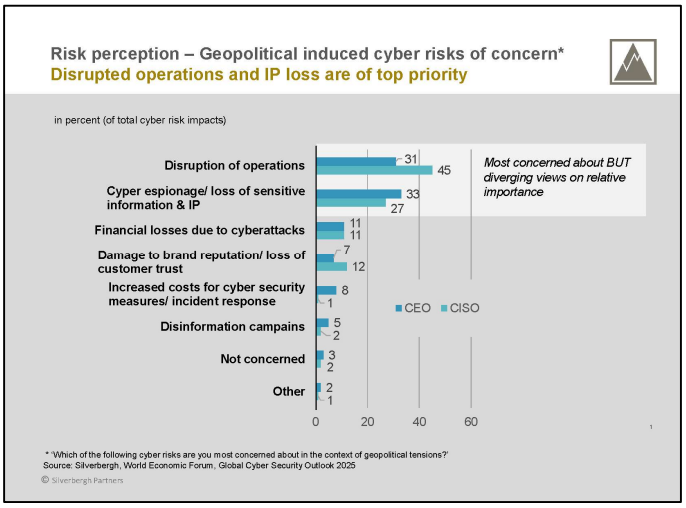
Companies now have to navigate how to deal with this new legal framework: Layer on a tedious, costly and potentially conflicting compliance procedures or integrate new requirements into existing systems relevant for established management routines.

Silverbergh Partners

VICCON CONSULTING – In cooperation with ...

Introduction

The NIS2 Directive[1] has been transposed into national law[2] by most EU member[3] and some EFTA countries. The Directives' objective is to protect businesses from increasing cyber risks *(see Appendix 1)*. Global annual damages from cyber risk events have more than tripled since 2020 reaching USD 10.5 tr by the end of 2025.[4] This meets the risk perception of senior executives who are especially concerned about operational disruptions and loss of IP. *(see exhibit)*.



Reducing companies' vulnerability is achieved by regulating cyber security risk management measures and capabilities. As such 'cyber security fitness', incident response and documentation are subject to fines in case of non-compliance. [5]

Liability may not be limited to entities. The Directive requires Members States to hold ' ... any natural person [acting as a legal representative of an essential entity] liable for breach of their duties to ensure compliance with this Directive'.[6] In Germany, the management board cannot delegate the NIS2 implementation to IT departments. Members of the management board are responsible for implementation, supervision and participation in frequent cyber security trainings. If compliance requirements are not met, they are personally liable not only in case of intent but also negligence.[7]

Likely pitfalls and potential opportunities

The Directive is written from a pure cyber perspective but does not elaborate on how to integrate into an existing company context. Implementing the NIS2 Directive requires some effort as requirements set out by the regulator are quite specific.

---

[1] European Parliament and Council; Directive on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), Brussels, 14 December 2022; Directive - 2022/2555 - EN - EUR-Lex

[2] By early 2026, 14 of the 27 member states have introduced national legislation plus Lichtenstein

[3] Germany: Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, Berlin, 5.12.2025; Bundesgesetzblatt Teil I - Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung - Bundesgesetzblatt

[4] Cybersecurity Ventures, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025" https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[5] Example Germany: BSIG § 32: Initial reporting/early warning: within 24h, detailed analysis of incident: within 72h, final report with root-cause analysis: within 30 days

[6] Art 32, 6

[7] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz - BSIG) § 38 BSIG - Einzelnorm

Likely pitfalls

- **'Boil the ocean'** – Get bogged down in detail, producing numerous documents to a very detailed level
- **'Compliance over relevance'** – Lose sight of priorities from a management point of view
- **'Duplication'** – Employ greenfield approach rather than aligning the new framework with existing procedures and structures i.e. Corporate Risk Management, IT-lead Cyber risk management; Finance, Insurance management, Business Continuity Management, Operations-lead supplier management (potentially supported by credit risk management), …
- **'Lack of effectiveness'** – New cyber risk measures are not adopted by the organisation and are not becoming part of the business and risk culture
- **'Excessive costs'** – Implementation and operating costs are disproportionate to the benefits as the implementation plan is not scoped appropriately. If measures prove not to be effective, additional risk costs will materialize as well

Potential opportunities

- **Upgrade existing frameworks & processes** increasing operational & financial resilience
- **Comply with new regulation** with limited effort
- **Vitalize 'management step childs'** i.e. supply chain resilience, business continuity management, risk-opportunity culture
- **Avoid duplication** and employee work overload
- **Improve risk adjusted bottom-line profitability**

NIS2 cyber risk requirements & interfaces

Numerous requirements companies have to comply with have been set out in NIS2 articles 20 and 21. However, companies have already established organizational structures and processes. Ignoring these and opting for a greenfield approach to achieve NIS2 compliance would be negligent and lead to less effective outcomes.

Overlaps of NIS2 demands with current organizational units and obligations are numerous *(see exhibits)*. Beyond IT, other units have already a role to support seamless management i.e.

- **Risk management** is the natural owner of the risk inventory and risk management methodology calculating and updating risk exposures
- **Operations & supply chain management** is most likely be affected by a risk event and can also contribute to risk mitigation (in most cases in the context of an existing business continuity plan) whereas credits risk management contributes to supplier management and pricing
- **Insurance management** does not only administer cyber security insurance policies but also (site/plant specific) business continuity policies
- **HR and HSE** are stakeholders if company staff is affected. This holds true not only if staffs' health is at risk but also if work schedules/ shifts need to be amended
- **Supply chain management and purchasing/ procurement** has a role one the production plan changes impacting in-/outbound shipments and supplies
- **Finance** and its' sub-functions beyond risk management must deal with all financial implications

NIS2 cyber risk requirements and interfaces – examples (1/2)
Numerous organizational interfaces and alignment needs

Cyber	Legacy/ non-cyber	+ General management
NIS2 requirements	**Key organizational interfaces**	**Key considerations, selected**
Mgmt. approval – cyber security RM measures & implementation	Risk management (CRO & board (risk committee))	Risk register Risk assessment methodology, currency of risk Risk appetite statement & risk bearing capacity Mitigation planning & insurance
Technical, operational and organizational measurer	Operations/ sites Supply chain management Purchasing/procurement	Risk governance/ risk ownership Continues/ ad-hoc processes Risk monitoring, early warning & prioritization
Measurers based on exposure & likelihood	Risk management Finance	Risk quantification & updates
Business continuity	Operations Risk management/ insurance management	Business continuity planning integration Interdependencies with existing BCP
Disaster recovery	Operations Supply chain management Insurance management Regulatory management Corporate communication HSE, Crisis mgmt. (committee), HR	Operations/ production plan Shift planning Supply chain schedule Revenue recognition & financial planning Regulator communication (mandatory?)
Supply chain security & supplier relations	Purchasing/ procurement Credit risk management Operations	Scheduling of shipments (inbound/ outbound) Supplier management & redundancies Inherent operational optionalities (operational & contractual)

CRM integration

NIS2 cyber risk requirements and interfaces – examples (2/2)
Numerous organizational interfaces and alignment needs

Cyber	Legacy/ non-cyber	+ General management
NIS2 requirements	**Key organizational interfaces**	**Key considerations, selected**
Human resource security	HSE, HR	Training Crisis notification & actions
Asset management	(Physical) asset management	Exposure by site, plant, type of machinery; interdependencies
Emergency communication	Regulatory management Corporate communications Shareholder relations HSE/ HR	Communication plan (concise across functions) & philosophy, channels Governance – spokesperson(s) Involvement/ role of external communication agency
Intermediate status update	Crisis mgmt. (committee) Corporate communication	Communication process (RACI?)

resulting from (ongoing) cyber risk management and potential events impacting financial plans, cash management, covenants negotiated by treasury and financial targets communicated to shareholders.

- **Corporate communication, regulatory management, shareholder relations** as well as HR and insurance management need to communicate with their respective stakeholder groups. These communications should be concise, and timing should be synchronized.
- **General management** is in the end responsible for implementation of cyber security measures and for managing potential cyber risk events. Therefore, it has to provide guidance, coordination and supervision.

How to approach the task

As discussed previously, a greenfield bottom-up approach will lead to flawed results as methodologies and processes will most likely not deliver desirable outcomes. Organizations structures will overlap, processes may not be aligned and methodologies may be conflicting.

A common flaw are risk assessment and quantification methodologies which are not in line with what is common practice in CRM. Risks cannot be aggregated, coherent risk coverage across different risk types and mitigation cannot be provided. Hence, employing a hybrid approach by mapping new requirements against existing organizational elements will deliver fast and fit-for-purpose results.

Summary and outlook

The new directive provides relevant guidance how to elevate cyber risk management to the next level. As such operational and financial stability of a company can be improved by at the same time ensuring regulatory compliance.

It depends on the companies approach how useful implementation outcomes will be.

Either new regulatory requirements lead to a tedious, costly and ineffective cyber risk management approach basically ticking off compliance check boxes.

Alternatively, the result is a concise cyber risk management in line with the established Corporate Risk Management (CRM) framework and broader management routines also stimulating targeted organizational and infrastructure upgrades along the way.

www.silverbergh.com

APPENDIX 1: Regulation

REGULATORY CONTEXT
NIS2 Directive[1]

Objectives
The directive aims to improve cyber security by expanding regulation beyond critical infrastructure into major industrial sectors.

Sectors subject to regulation
The scope of companies included in the regulation comprises companies with the following criteria:

- **Sectors**
  - **Annex 1**: Energy, Water/wastewater, Digital Infrastructure, Transport, Health, Transport, Banking/Financial market infrastructure, ICT services (B2B), Space
  - **Annex 2**: Waste management, Postal & courier services, Food, Public admin, Chemicals, Manufacturing, Digital providers, Research
- **Size**
  - **Important entities:** Annex 1 companies; < EUR 50 m revenue, BS < EUR 43 m, <250 employees**;** Annex 2 companies revenue > 10 EUR m or 50 employees
  - **Essential entities:** Annex 1 companies; > revenues EUR 50 m OR BS > EUR 43 m OR >250 employees

Requirements
The directive asks to create organizational structures, processes, methodology and policies including

- **Risk management:** Analytics, decision making & treatment
- **Incident response:** Processes, responsibilities and actions; 24 h instant reporting requirement[5]
- **Business continuity:** Backup strategies and recovery plans
- **Supply chain security:** evaluation of suppliers and contractors
- **Training:** Frequent training and awareness programs

Reporting
- Registration of important and essential entities with domain names
- Incident reporting[5]

Costs of non-compliance
As risk exposures increase, costs of risks materializing need to be prevented. Recent history shows that these costs can be substantial. The new legislation can be instrumental to achieve this.

From a legal perspective, fines of non-compliance comprise ...

ENTITY LEVEL

- **Essential entities:** EUR 10 m or 2% of global annual revenues
- **Important entities:** EUR 7 m or 1.4% of global annual revenues

INDIVIDUAL LEVEL

- Liability of individual executive board members/ legal representatives in case of intent or negligence (not capped)