
SBA
Research

Stefan Jakoubi

Head of Professional Services, CISO

Prokurist

- Since 18 years in “the” InfoSec field
  - Main **focus on security governance**
- **CISO** of the research center SBA Research
  - **Scientific & Applied Research** (maybe NIS-2)
  - **Professional Services** = ISO27001 certified & Qualified Body according to the Austrian NIS Act
- **Head of Professional Services** = cost-aware ;-)

From October 18th, it will be "compliant" or "non-compliant"

NIS-2 Directive

- **Objective:** This directive aims to build **cybersecurity capabilities across the Union** and **to mitigate threats to network and information systems which provide essential services in key sectors.**

- Further development of NIS-1 (since 2018)
  - NIS-1 in Austria → ~100 Companies that provide essential services
  - NIS-2 in Austria → ~6.000 companies + supply chain

NIS-2 Key Sectors

Focus on Medium Sized and Large Enterprises

Important Entities

- Postal and courier services
- Waste management
- Manufacturing, production and distribution of chemicals
- Production, processing and distribution of food
- Manufacturing
  - Manufacturing of machinery
- Digital providers
- Research

Essential Entities

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Waste water
- Digital infrastructure
- ICT service management (B2B)
- Public administration
- Space

Remark: Small Enterprises only if „key role for society“

NIS-2 Directive

Strict Management Liabilities

Article 20

Governance

1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.

The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.

2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

NIS-2 Directive

Cybersecurity Risk-Management as Fundamental Pillar

Article 21

Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2555

NIS-2 Directive

Risk-Management Measures

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

NIS-2 Law Appendix 3

Risikomanagementmaßnahmen-Bereiche	
1.	Leitungsorgane
a.	Rollen und Verantwortlichkeiten der Leitungsorgane
2.	Sicherheitsrichtlinien
a.	Sicherheitsrichtlinien
b.	Funktionen, Aufgaben und Verantwortlichkeiten
3.	Risikomanagement
a.	Risikomanagementrichtlinie und -prozess
b.	Beurteilung der Effektivität von Risikomanagementmaßnahmen
c.	Überwachung der Einhaltung von Vorgaben
d.	Unabhängige Überprüfungen
4.	Verwaltung von Vermögenswerten
a.	Inventarisierung von Vermögenswerten
b.	Klassifikation von Vermögenswerten
c.	Handhabung von Vermögenswerten
d.	Umgang mit Wechseldatenträger
e.	Rücknahme oder Löschung von Vermögenswerten
5.	Personalwesen
a.	Sicherheit im Personalwesen
b.	Hintergrundüberprüfung
c.	Verfahren bei Beendigung oder Wechsel des Beschäftigungsverhältnisses
d.	Disziplinarmaßnahmen
6.	Grundlegende Cyberhygienemaßnahmen und Cybersicherheitsschulungen
a.	Bewusstseinsschaffung und Cyberhygiene
b.	Cybersicherheitsschulungen
7.	Sicherheit von Lieferketten
a.	Richtlinie zur Sicherheit von Lieferketten
b.	Lieferantenverzeichnis
8.	Zugangssteuerung
a.	Zugangssteuerungsrichtlinie
b.	Verwaltung von Zugriffsberechtigungen
c.	Privilegierte und administrative Zugänge
d.	Systeme und Anwendungen zur Systemadministration
e.	Identifikation
f.	Authentifikation
g.	Multi-Faktor-Authentifikation

9.	Sicherheit bei Beschaffung, Entwicklung, Betrieb und Wartung
a.	Konfigurationsmanagement
b.	Änderungsmanagement und Wartung
c.	Umgang mit Schwachstellen und deren Offenlegung
d.	Sicherheitstests
e.	Patchmanagement
f.	Sicherheit bei der Beschaffung von Dienstleistungen, Systemen und Produkten
g.	Sichere Softwareentwicklung
h.	Netzwerksegmentierung
i.	Netzwerksicherheit
j.	Schutz vor bösartiger und unautorisierter Software
10.	Kryptographie
a.	Kryptographierichtlinie
11.	Umgang mit Cybersicherheitsvorfällen
a.	Richtlinie zum Umgang mit Cybersicherheitsvorfällen
b.	Überwachung und Protokollierung
c.	Meldung von Ereignissen
d.	Erhebung und Klassifikation von Ereignissen
e.	Reaktion auf Cybersicherheitsvorfällen
f.	Erkenntnisse nach Cybersicherheitsvorfällen
12.	Betriebskontinuitäts- und Krisenmanagement
a.	Betriebskontinuitätsmanagement und Notfallwiederherstellungspläne
b.	Backup-, Redundanz- und Wiederherstellungsmanagement
c.	Krisenmanagement
13.	Umgebungsbezogene und physische Sicherheit
a.	Sicherheitsperimeter und physische Zutrittskontrollen
b.	Schutz vor umgebungsbezogenen Gefährdungen
c.	Versorgungseinrichtungen

NIS-2 Compliance Planning

Check existing Standards & Best-Practises

NIS-2 Directive

18.10.2024

NIS-2 Law

Governance
ISMS – Security processes

Training
Management bodies & employees

TOMs
Technical, operational & organizational measures

Article 21

Cybersecurity risk-management measures

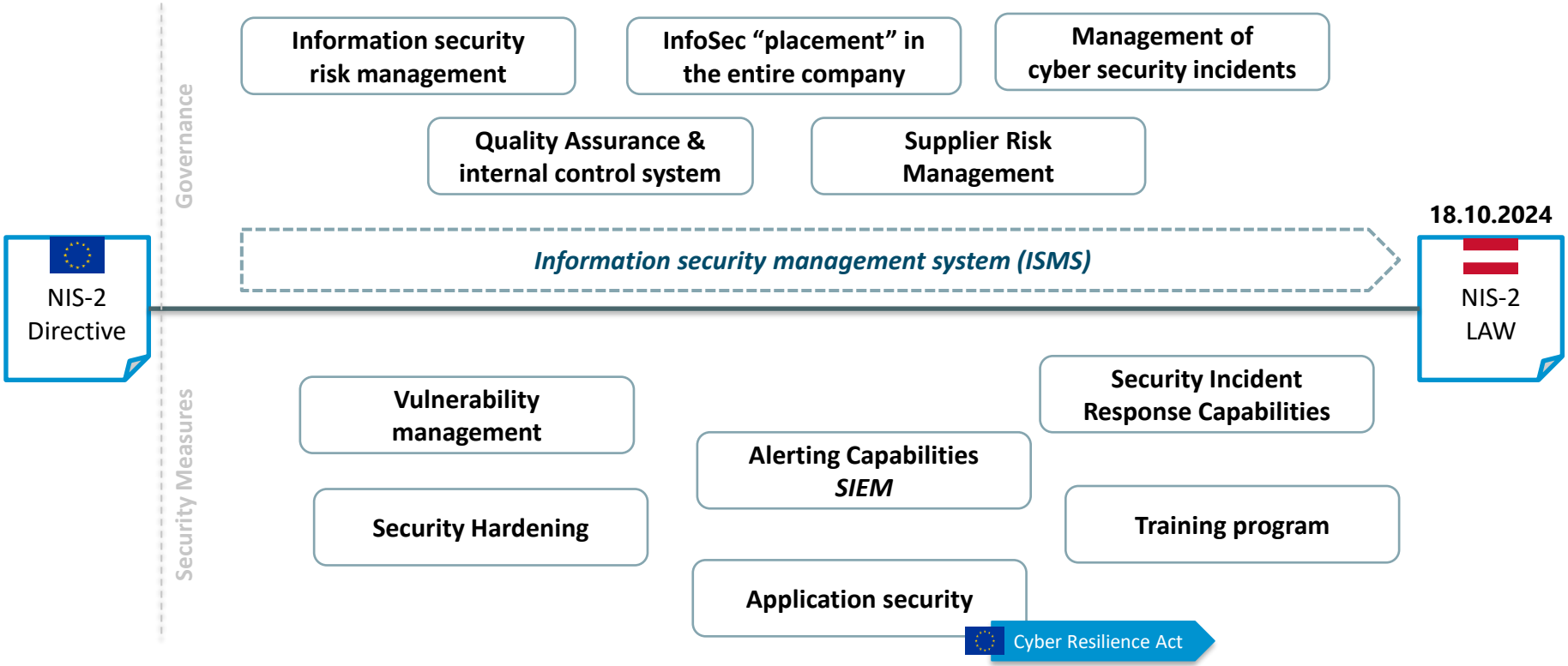
1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

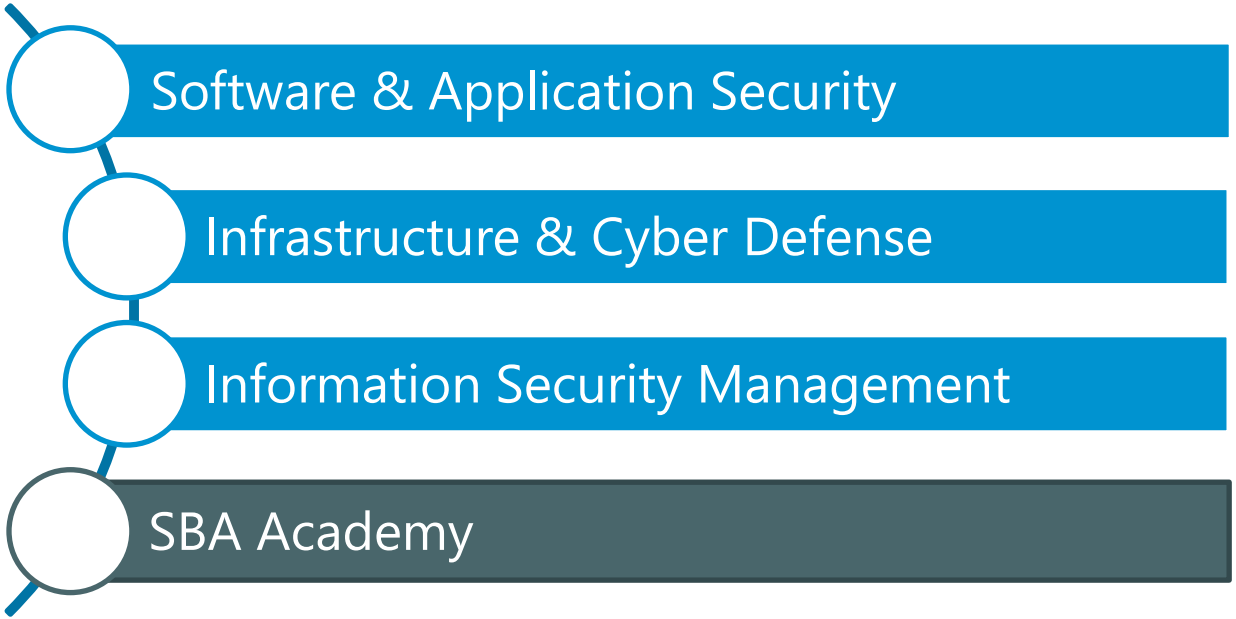
Hint: check ISO27001 & ISO27002 for preparation!

NIS-2 Challenges for SME

Selected topics with common cyber security weaknesses

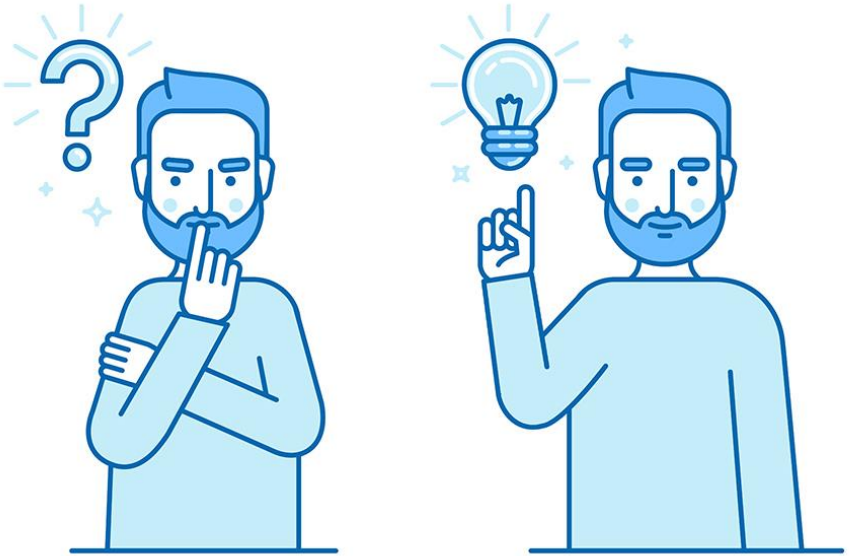


SBA Research – Professional Services



https://www.sba-research.org/professional-services

Questions & Discussion



Stefan Jakoubi

Head of Professional Services, CISO

Prokurist

SBA Research

Floragasse 7, 1040 Wien

+43 660 510 20 40

sjakoubi@sba-research.org

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie

Bundesministerium Arbeit und Wirtschaft

FFG Forschung wirkt.

wirtschaftsagentur wien

Für die Stadt Wien

European Commission

FWF Österreichischer Wissenschaftsfonds

netidee FÖRDERUNGEN