ECCO

European Cybersecurity COmmunity

ECCO Community Group on Trusted Supply Chains

Knowledge-Sharing Webinar: Organisational and Operation Security in Trusted Supply Chains

March 19 2024

Agenda

- Introduction to ECCO Community Group on Trusted Supply Chains and Webinar (5 Min)

- Organisational Security aspects of the Supply Chain Security (20 min)

- Supply chains from a hardware perspective (10 min)

- Open Q&A and discussion (10 min)

ECCO

European Cybersecurity COmmunity

ECCO Community Group on Trusted Supply Chains

Introduction

José Luis Hernández Ramos

March 19 2024

ECCO Community Working Groups

- Road-mapping
- Startups/Scaleups - SMEs support
- Human factors
- Skills
- Synergies on cybersecurity for Civilian and Space applications
- **Trusted supply chains**
    - **Chairs: Antonio Skarmeta and José Luis Hernández Ramos**
    - Participants: development of a "proto-community" based on the initial list of experts from ECSO and Pilots, and growing with additional people
    - Objectives
        - Build community of experts on trusted supply chains and Strengthening Trusted and Resilient Supply Chain in Europe
        - Facilitate trusted information sharing about threats (to support prevention and response)
        - Propose a strategy, planning and recommendations to support the NCCs in the implementation of the Strategic Agenda's Action Plan

ECCO Community Group on Trusted Supply Chains

- Relationship with ECCC strategic agenda [1]:

Increase the resilience of essential and important entities defined in NIS2 ***including their digital supply chain against cyber threats****, in line with the CRA and NIS2 directive. Specific attention goes to emerging technologies identified in The EU's Cybersecurity Strategy for the Digital Decade (i.e. cloud, 5G, IoT, blockchain), as well as underlying infrastructure resilience of secure European DNS servers with embedded security and privacy, support to European trust service providers supplying certificates and the manufacturing and adoption of secure Galileo PRS time and position signal receiving infrastructure*

[1] https://cybersecurity-centre.europa.eu/system/files/2023-03/20230224%20-%20ECCC%20Strategic%20Agenda%20with%20cover.pdf

ECCO Community Group on Trusted Supply Chains

- Some initial topics
    - Threats identification/prioritization and risk management for trusted supply chains Current landscape of standardization efforts (proposed and/or in use) around trusted supply chains
    - Identification of minimum security requirements and cyber risk rating for providers/suppliers
    - Existing best practices and national experiences around trusted supply chains
    - Practical aspects and challenges for the implementation of NIS2

Planned webinars

- This event is part of a webinar series focused on European cybersecurity supply chain.

- Initial list of webinars
  - Organisational and Operation Security in Trusted Supply Chains (today)
  - Certification in the lifecycle
  - Methodology for security of supply chains

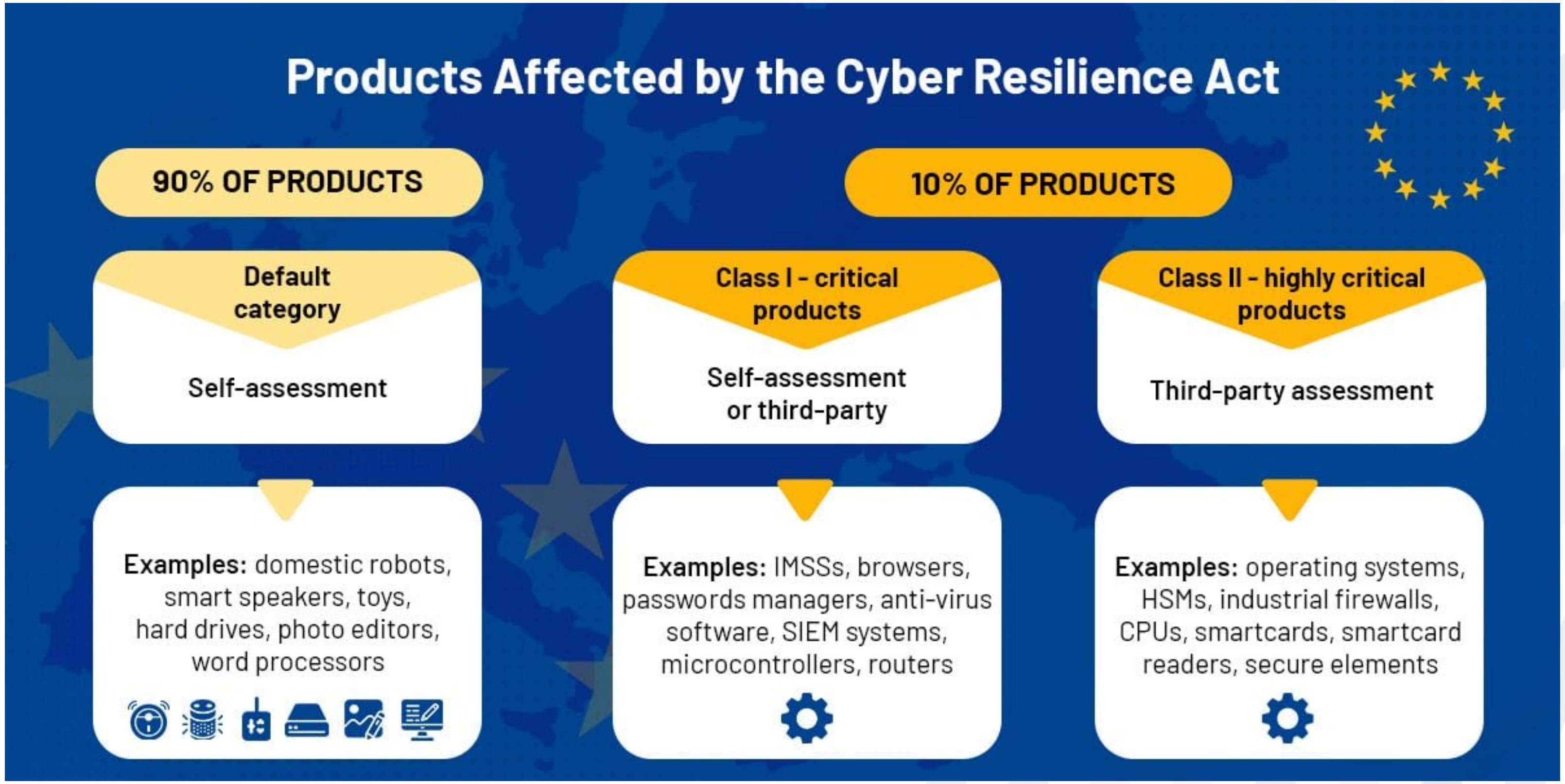
Community Group on Trusted Supply Chains – Organisational and Operation Security in Trusted Supply Chains

ECCO Webinar 19.3.2024

Co-funded by the European Union

Most regulatory efforts in Europe focus on product security

Which is important...



Products Affected by the Cyber Resilience Act

90% OF PRODUCTS

Default category

Self-assessment

Examples: domestic robots, smart speakers, toys, hard drives, photo editors, word processors

10% OF PRODUCTS

Class I - critical products

Self-assessment or third-party

Examples: IMSSs, browsers, passwords managers, anti-virus software, SIEM systems, microcontrollers, routers

Class II - highly critical products

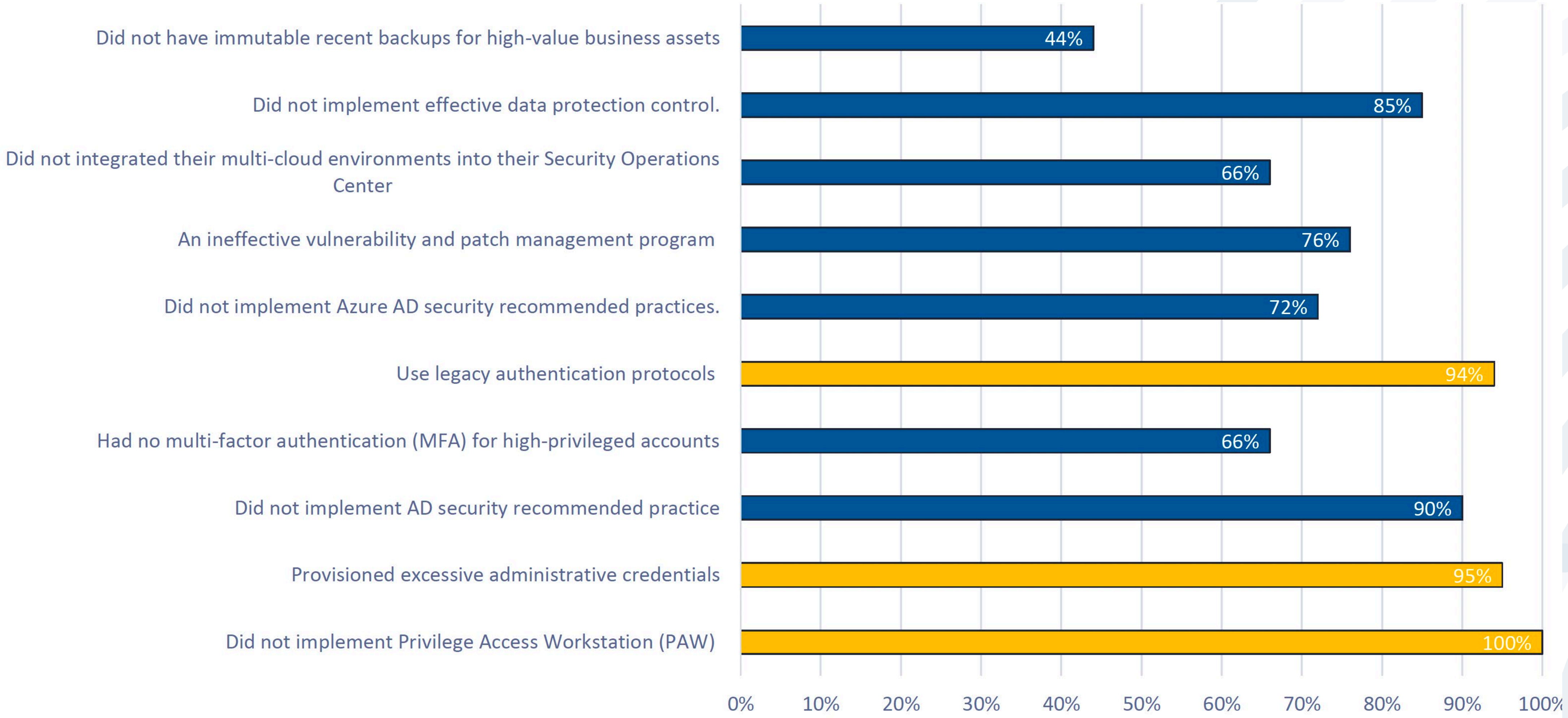
Third-party assessment

Examples: operating systems, HSMs, industrial firewalls, CPUs, smartcards, smartcard readers, secure elements

... but it leaves out of consideration the security of the providers themselves

Co-funded by the European Union

The reality of the supply market: Reasons for successful breaches

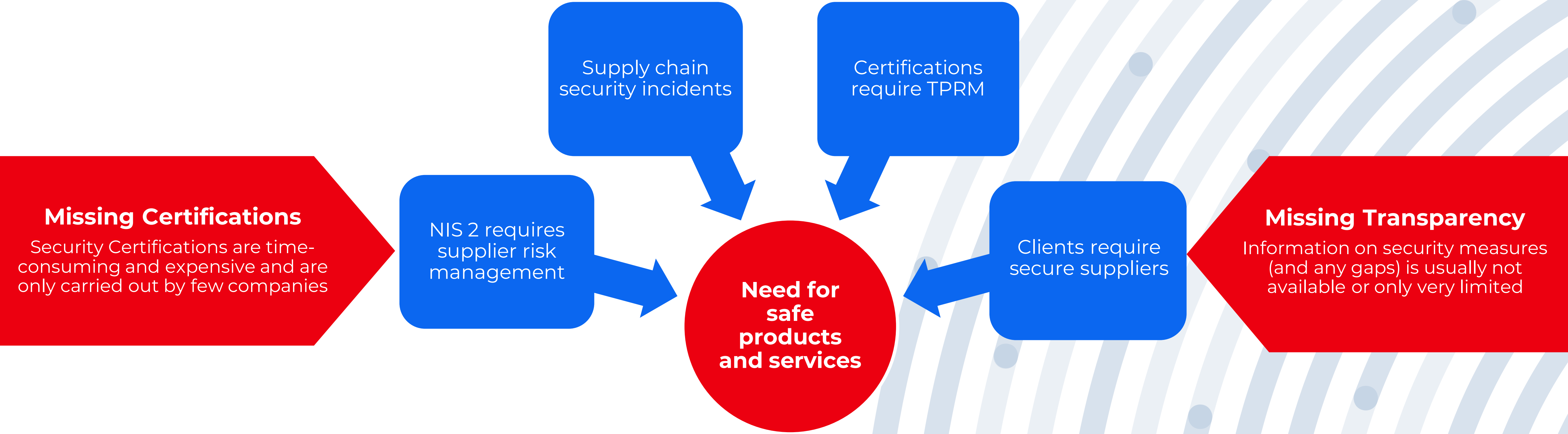


Source: Microsoft, RSA Conference 2023

Co-funded by the European Union

A supplier without organisational security cannot deliver secure products and services

Cyber attacks in the supply chain are a widely unsolved problem for most companies. With NIS 2* at the latest, it will become mandatory for thousands of companies in Austria and Europe to solve this problem.



Missing Certifications

Security Certifications are time-consuming and expensive and are only carried out by few companies

NIS 2 requires supplier risk management

Supply chain security incidents

Certifications require TPRM

Clients require secure suppliers

Need for safe products and services

Missing Transparency

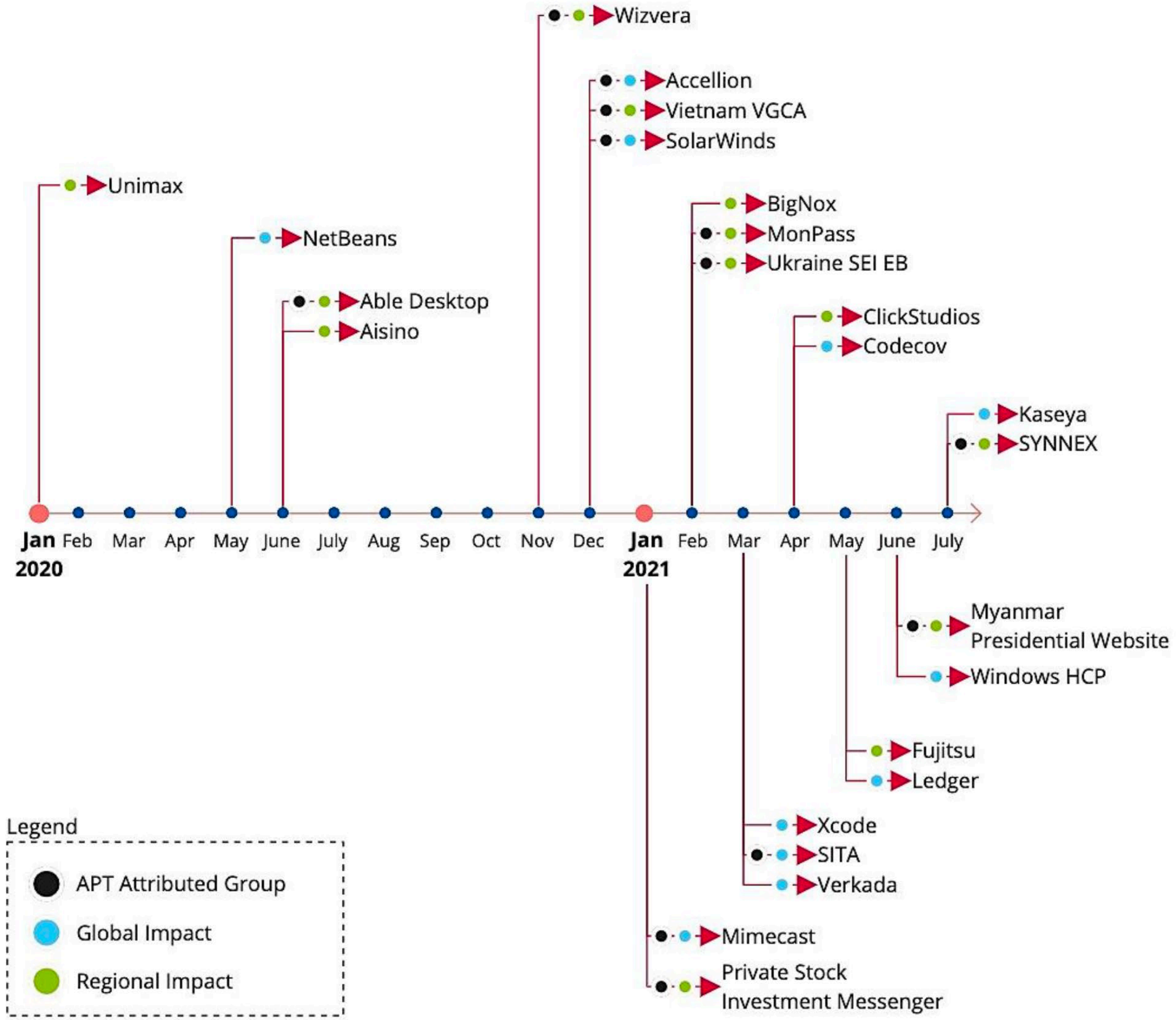
Information on security measures (and any gaps) is usually not available or only very limited

* Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive): EU Directive, which prescribes mandatory cyber security standards for critical and important infrastructure companies. This directive will come into effect in Austria and other member states at the latest by 18.10.2024.

Co-funded by
the European Union

ENISA Report Threat Landscape for Supply Chain Attacks

Summary of the supply chain attacks identified, analysed and validated from Jan 2020 to July 2021

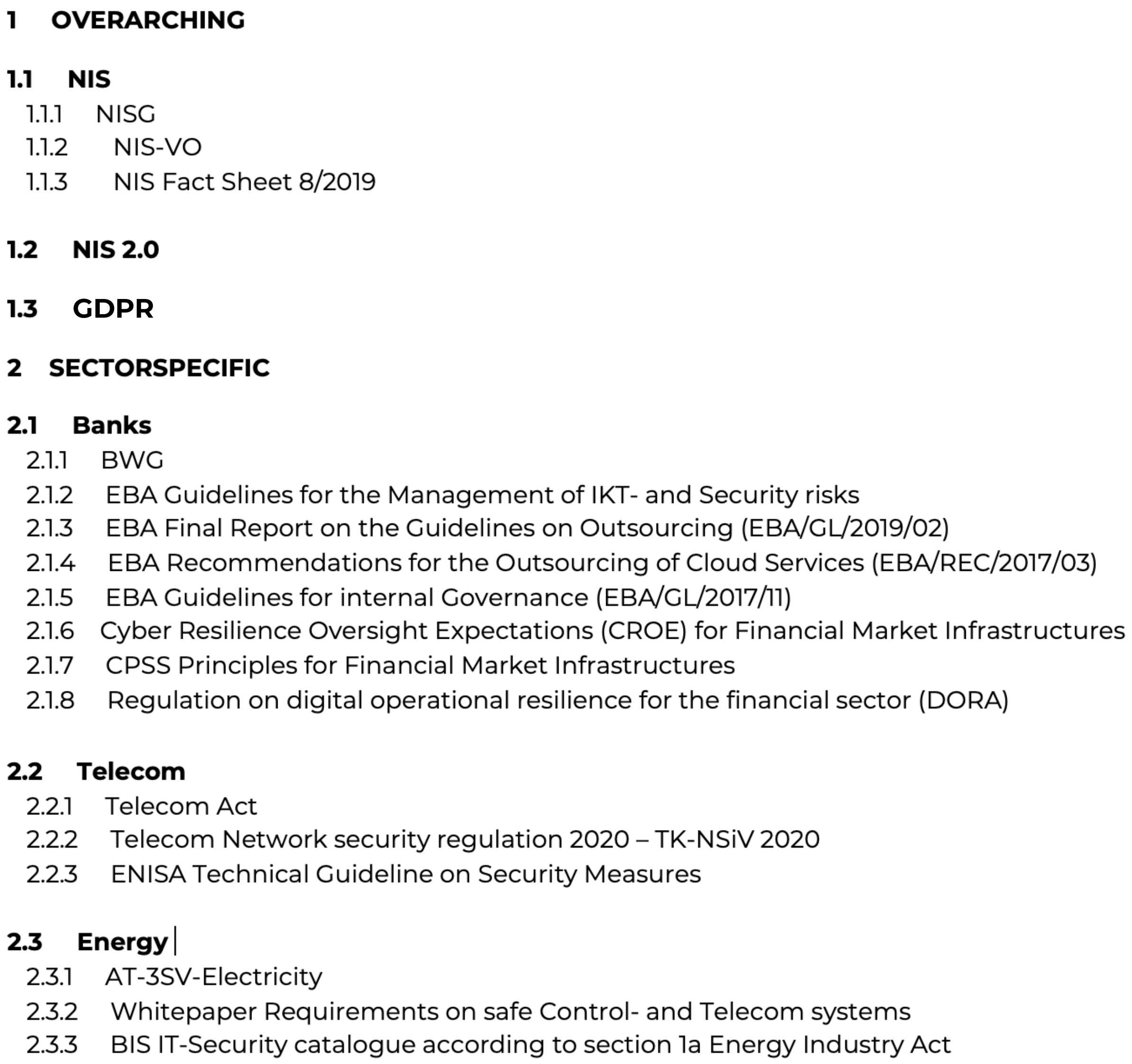


- *Around 50% of the attacks were attributed to well-known APT groups by the security community.*
- *Around 62% of the attacks on customers took advantage of their trust in their supplier.*
- *In 62% of the cases, malware was the attack technique employed.*
- *When considering targeted assets, in 66% of the incidents attackers focused on the suppliers' code in order to further compromise targeted customers.*
- *Around 58% of the supply chain attacks aimed at gaining access to data (predominantly customer data, including personal data and intellectual property) and around 16% at gaining access to people.*
- *Organizations need to update their cybersecurity methodology with supply chain attacks in mind and to incorporate all their suppliers in their protection and security verification.*

Quelle: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Co-funded by the European Union

Laws and regulations that require baseline security



1 OVERARCHING

1.1 NIS

- 1.1.1 NISG
- 1.1.2 NIS-VO
- 1.1.3 NIS Fact Sheet 8/2019

1.2 NIS 2.0

1.3 GDPR

2 SECTORSPECIFIC

2.1 Banks

- 2.1.1 BWG
- 2.1.2 EBA Guidelines for the Management of IKT- and Security risks
- 2.1.3 EBA Final Report on the Guidelines on Outsourcing (EBA/GL/2019/02)
- 2.1.4 EBA Recommendations for the Outsourcing of Cloud Services (EBA/REC/2017/03)
- 2.1.5 EBA Guidelines for internal Governance (EBA/GL/2017/11)
- 2.1.6 Cyber Resilience Oversight Expectations (CROE) for Financial Market Infrastructures
- 2.1.7 CPSS Principles for Financial Market Infrastructures
- 2.1.8 Regulation on digital operational resilience for the financial sector (DORA)

2.2 Telecom

- 2.2.1 Telecom Act
- 2.2.2 Telecom Network security regulation 2020 – TK-NSiV 2020
- 2.2.3 ENISA Technical Guideline on Security Measures

2.3 Energy

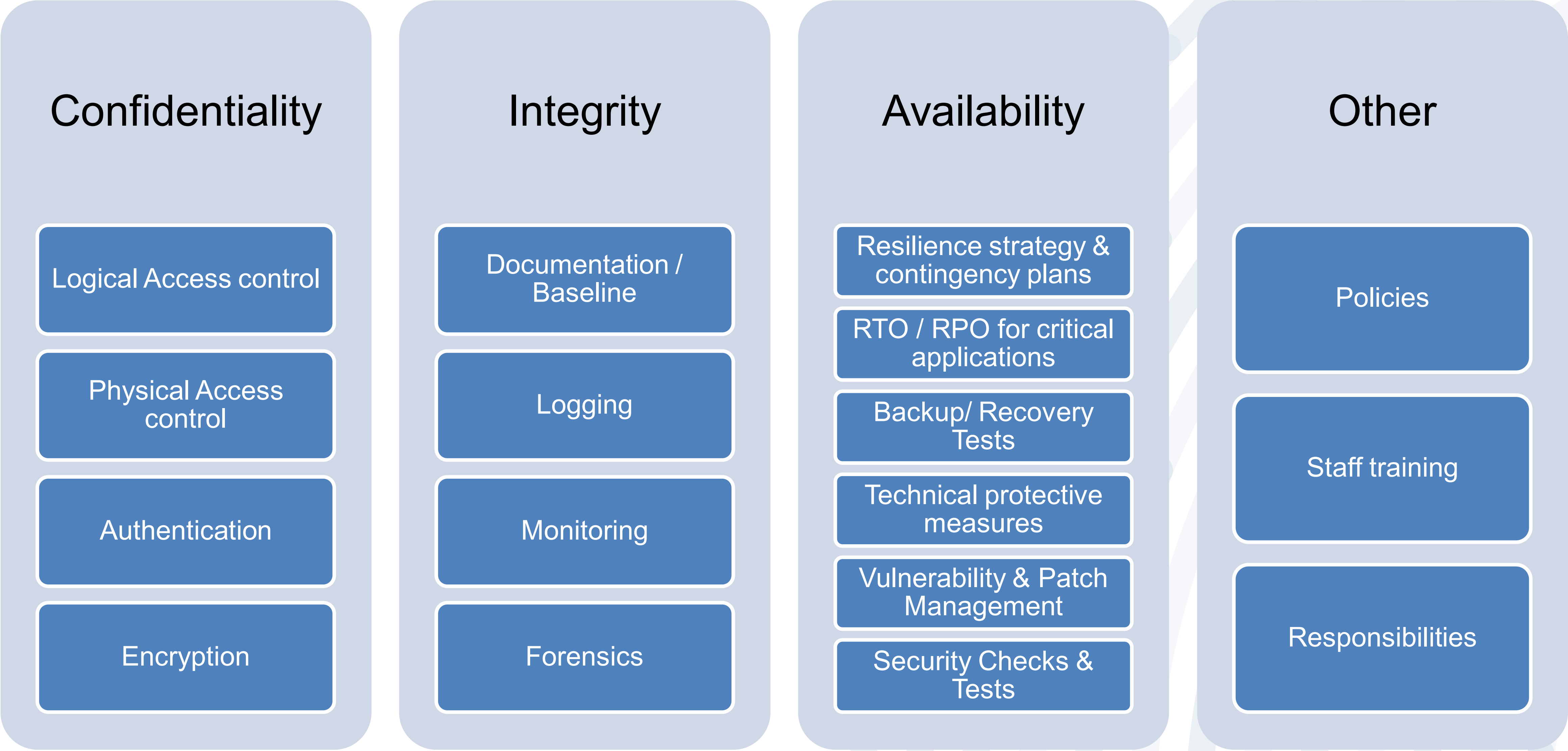
- 2.3.1 AT-3SV-Electricity
- 2.3.2 Whitepaper Requirements on safe Control- and Telecom systems
- 2.3.3 BIS IT-Security catalogue according to section 1a Energy Industry Act

"Contracts and service agreements with providers (outsourcing providers, group companies or third party providers) must include the following:
(a) appropriate and proportionate information security objectives and measures, including minimum cyber security requirements [...].
Service providers must be monitored with regard to safety objectives, measures and fulfilment of the agreed performance."

EBA Guidelines on ICT and Security Risk Management

Co-funded by
the European Union

Basic security requirements that every organisation should meet



Confidentiality

- Logical Access control
- Physical Access control
- Authentication
- Encryption

Integrity

- Documentation / Baseline
- Logging
- Monitoring
- Forensics

Availability

- Resilience strategy & contingency plans
- RTO / RPO for critical applications
- Backup/ Recovery Tests
- Technical protective measures
- Vulnerability & Patch Management
- Security Checks & Tests

Other

- Policies
- Staff training
- Responsibilities

Co-funded by the European Union

CIS Top 18 Security Controls Overview

CONTROL	Title	Safeguards	IG1	IG2	IG3
01	Inventory and Control of Enterprise Assets	5	2/5	4/5	5/5
02	Inventory and Control of Software Assets	7	3/7	6/7	7/7
03	Data Protection	14	6/14	12/14	14/14
04	Secure Configuration of Enterprise Assets and Software	12	7/12	11/12	12/12
05	Account Management	6	4/6	6/6	6/6
06	Access Control Management	8	5/8	7/8	8/8
07	Continuous Vulnerability Management	7	4/7	7/7	7/7
08	Audit Log Management	12	3/12	11/12	12/12
09	Email and Web Browser Protections	7	2/7	6/7	7/7
10	Malware Defenses	7	3/7	7/7	7/7
11	Data Recovery	5	4/5	5/5	5/5
12	Network Infrastructure Management	8	1/8	7/8	8/8
13	Network Monitoring and Defense	11	0/11	6/11	11/11
14	Security Awareness and Skills Training	9	8/9	9/9	9/9
15	Service Provider Management	7	1/7	4/7	7/7
16	Applications Software Security	14	0/14	11/14	14/14
17	Incident Response Management	9	3/9	8/9	9/9
18	Penetration Testing	5	0/5	3/5	5/5

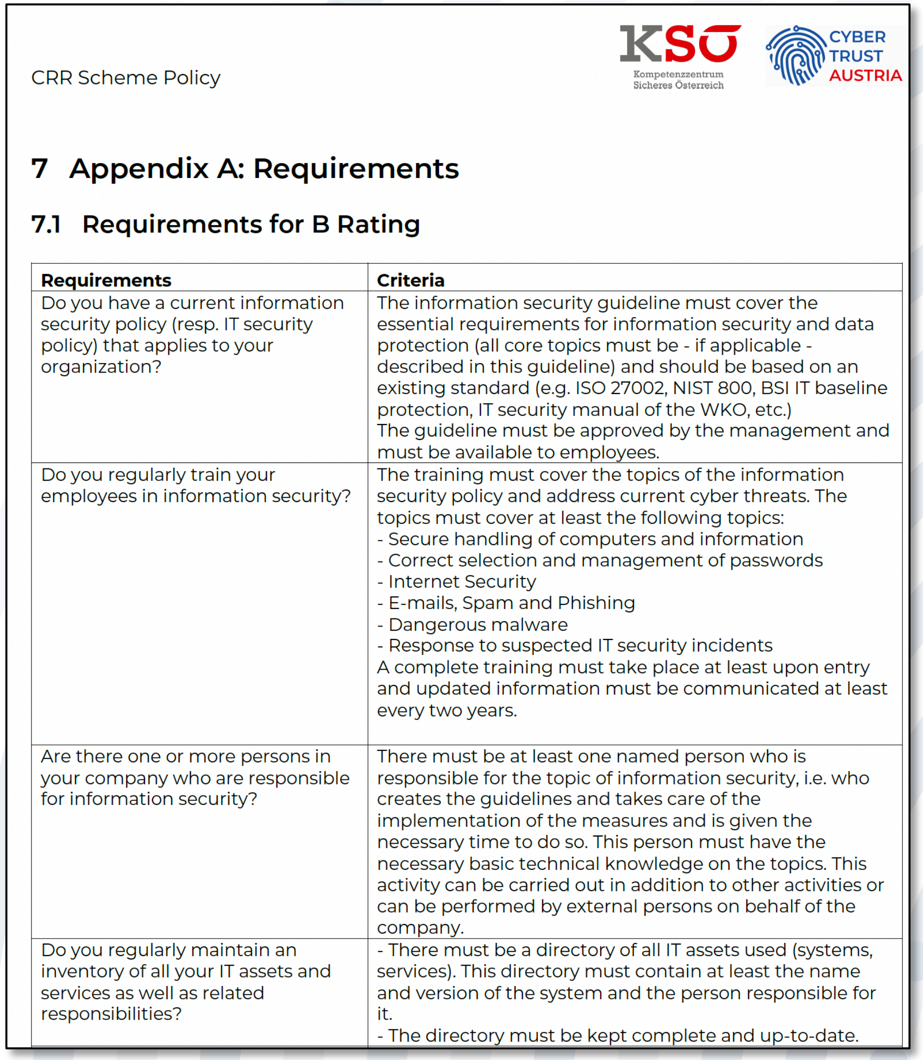
https://www.cisecurity.org/controls/cis-controls-list

Co-funded by the European Union

The Austrian Cyber Risk Rating Scheme for Baseline Security

- 25 Requirements for baseline controls:
  - 14 Basic requirements (B)
  - 11 (additional) more advanced requirements (A)
- Covers both technical and organizational controls
- Three levels of assurance:
  - Standard (Basic, Validated self-assessment)
  - Silver (Advanced, Validated self-assessment)
  - Gold (Advanced, Audit)
- Fulfils the requirements of Third Party Risk Management according the Austrian NIS fact sheet

https://kompetenzzentrum-sicheres-oesterreich.at/wp-content/uploads/2023/09/CRR-Schema-Policy-2023-final.pdf



CRR Scheme Policy

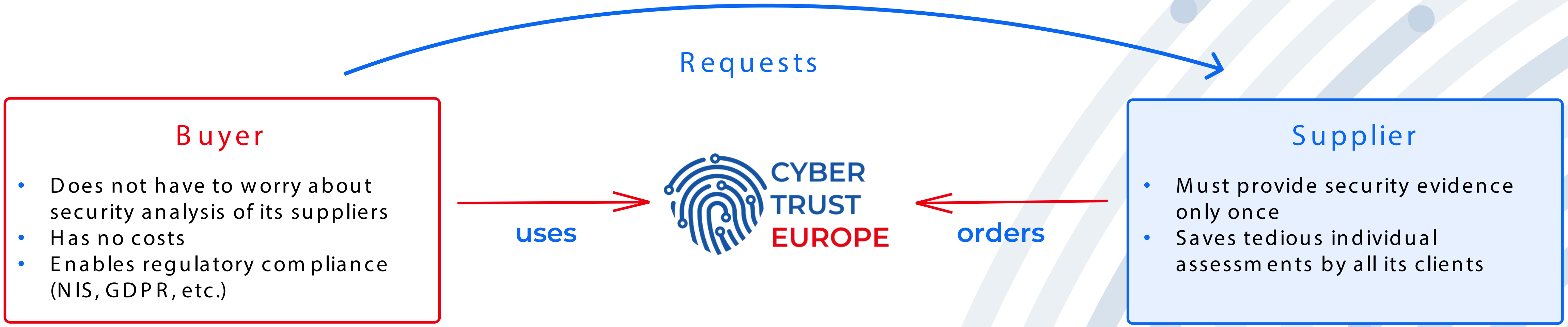
7 Appendix A: Requirements

7.1 Requirements for B Rating

Requirements	Criteria
Do you have a current information security policy (resp. IT security policy) that applies to your organization?	The information security guideline must cover the essential requirements for information security and data protection (all core topics must be - if applicable - described in this guideline) and should be based on an existing standard (e.g. ISO 27002, NIST 800, BSI IT baseline protection, IT security manual of the WKO, etc.) The guideline must be approved by the management and must be available to employees.
Do you regularly train your employees in information security?	The training must cover the topics of the information security policy and address current cyber threats. The topics must cover at least the following topics: - Secure handling of computers and information - Correct selection and management of passwords - Internet Security - E-mails, Spam and Phishing - Dangerous malware - Response to suspected IT security incidents A complete training must take place at least upon entry and updated information must be communicated at least every two years.
Are there one or more persons in your company who are responsible for information security?	There must be at least one named person who is responsible for the topic of information security, i.e. who creates the guidelines and takes care of the implementation of the measures and is given the necessary time to do so. This person must have the necessary basic technical knowledge on the topics. This activity can be carried out in addition to other activities or can be performed by external persons on behalf of the company.
Do you regularly maintain an inventory of all your IT assets and services as well as related responsibilities?	- There must be a directory of all IT assets used (systems, services). This directory must contain at least the name and version of the system and the person responsible for it. - The directory must be kept complete and up-to-date.

Co-funded by the European Union

This creates a win-win situation for customers and suppliers



Requests

Buyer

- Does not have to worry about security analysis of its suppliers
- Has no costs
- Enables regulatory compliance (NIS, GDPR, etc.)

uses

CYBER TRUST EUROPE

orders

Supplier

- Must provide security evidence only once
- Saves tedious individual assessments by all its clients

- Solving the compliance problem of NIS 2 companies for Supplier Risk Management
- Low-barrier approach to demonstrating baseline security, also suitable for SMEs
- Minimum standard accepted by the regulator
- Suppliers will spare time-consuming individual assessments
- Free complete solution for companies affected by NIS 2
- More transparency in the cybersecurity market in Austria & Europe

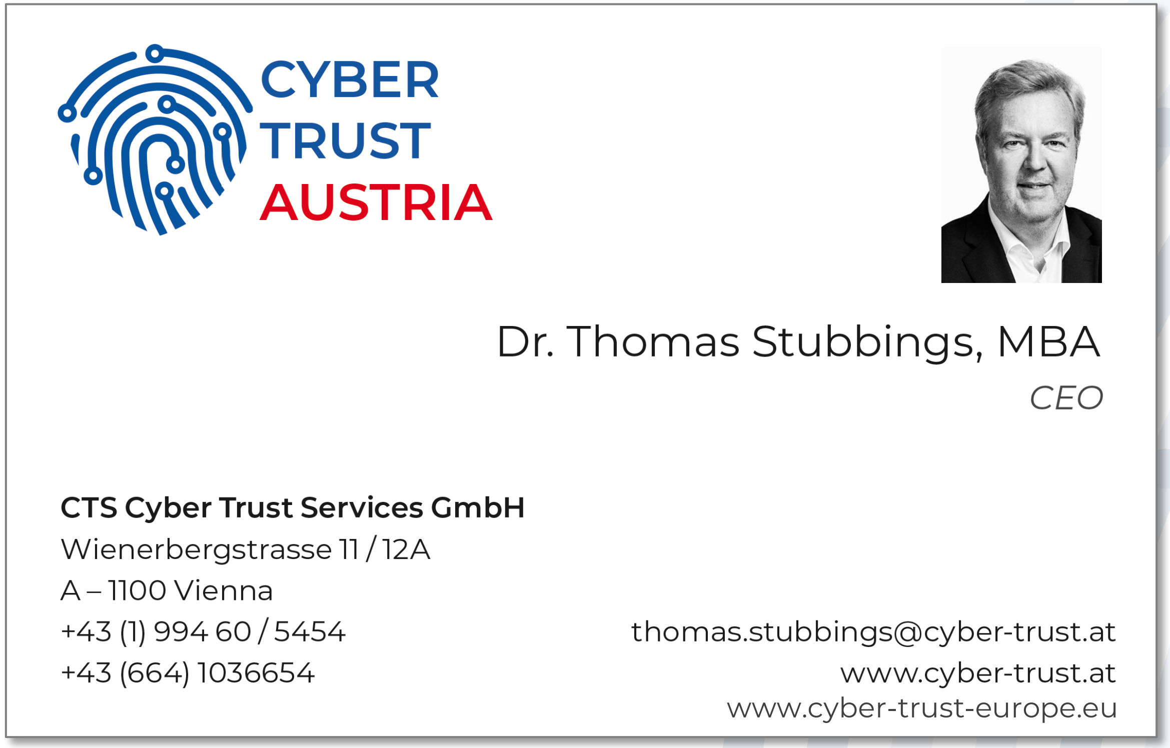
Co-funded by the European Union

Summary

- A low barrier entry level “certification” is urgently required by the market in order to scale the broadness of necessary market transparency
- Pure “outside-in” rating models do not provide adequate solidity of assertion (and will not be accepted by authorities)
- *Validation* creates the quality in the self-assessment process
- Many SMEs still struggle with the most basic requirements of cybersecurity
- Low barrier support is required to prepare SMEs for the requirements
- Other baseline schemes start to evolve – cross-reference and mutual recognition required

Co-funded by
the European Union

Your contact



CYBER
TRUST
AUSTRIA

Dr. Thomas Stubbings, MBA

CEO

CTS Cyber Trust Services GmbH
Wienerbergstrasse 11 / 12A
A – 1100 Vienna
+43 (1) 994 60 / 5454
+43 (664) 1036654

thomas.stubbings@cyber-trust.at
www.cyber-trust.at
www.cyber-trust-europe.eu

Co-funded by
the European Union

ECCO

European Cybersecurity COmmunity

Supply chain security

A Hardware Perspective

Matthias Hiller (Fraunhofer AISEC)

Drivers for implementing trusted electronics

Intrinsic drivers

- Differentiation
  (between competitors)
- Reputation loss
  (protect against incidents)
- Protection of the business
  (in case of incidents)

Extrinsic drivers

- Regulation
  (e.g. Common Criteria, CRA)
- Standardization
  (e.g. 62443, requirements from OEMs)
- Insurance companies

Definition: trusted electronics

Hardware must

1. meet high levels of quality and reliability

Reliable operation in the field over its full lifetime.

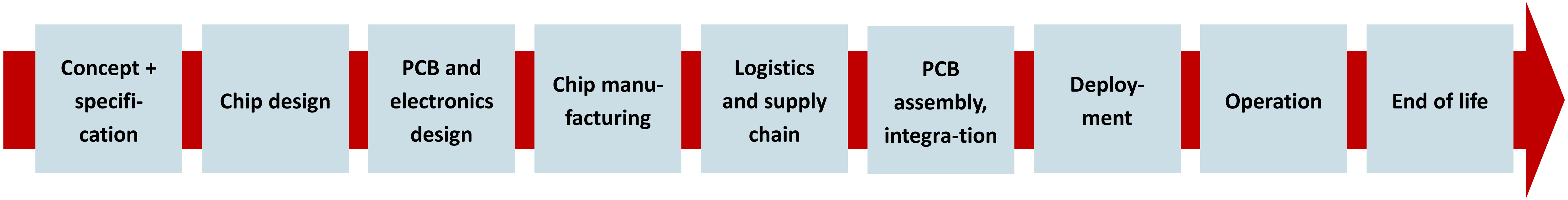
2. comply to a known and complete specification

Functionality cannot be altered from the specification.

3. be sufficiently hardened against attacks

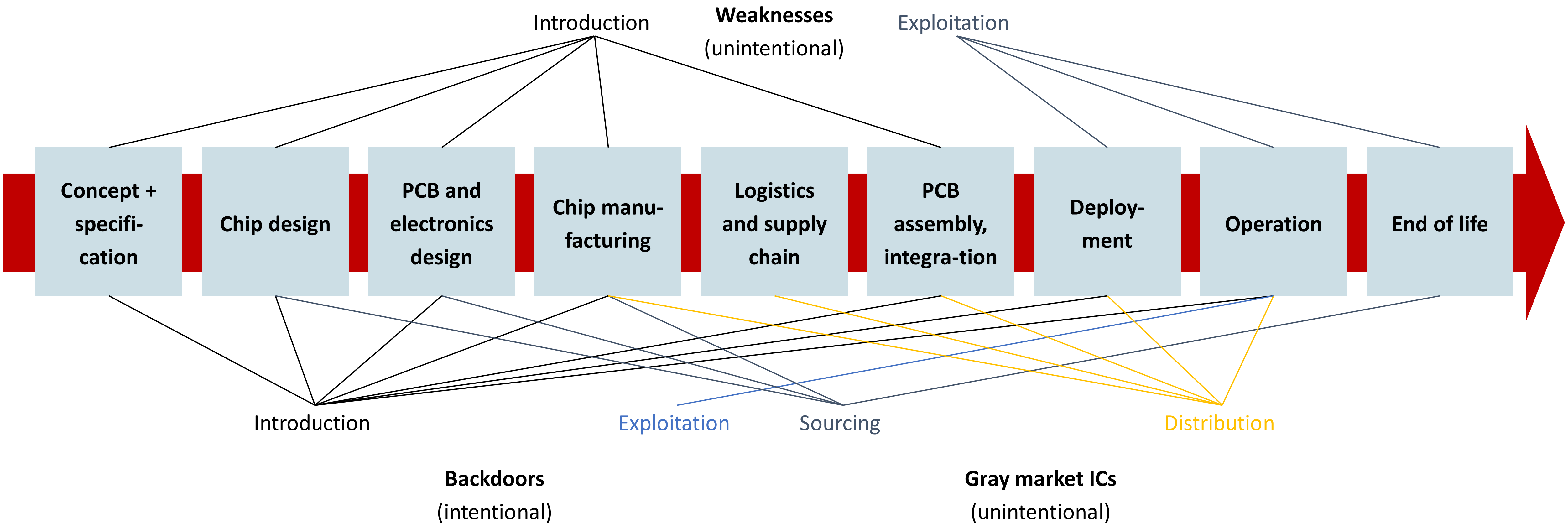
Mechanisms to ensure security and avoid vulnerabilities.

Electronics value chain



- Concept + specification
- Chip design
- PCB and electronics design
- Chip manufacturing
- Logistics and supply chain
- PCB assembly, integra-tion
- Deployment
- Operation
- End of life

Vulnerabilities along the value chain



Way forward

- Increase resilience of supply chains
- Research on new technologies
- Combination of market demand + regulation
- Awareness and Education

Sources:

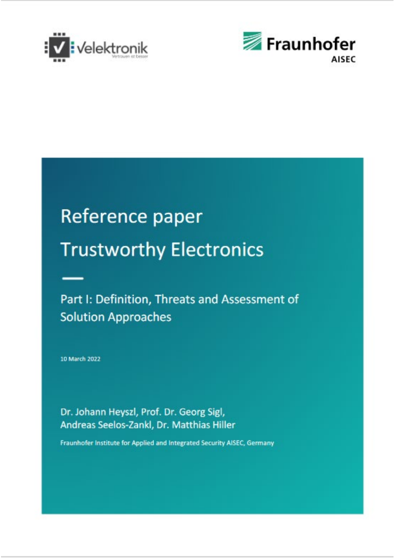
European Commission

Study on Trusted Electronics

An overview over requirements, technologies and initiatives towards more trusted electronics

Written by Matthias Hiller and Johanna Baehr, Fraunhofer AISEC
November 2023

Fraunhofer AISEC



Velektronik Vertrauen ist besser

Fraunhofer AISEC

Reference paper

Trustworthy Electronics

Part I: Definition, Threats and Assessment of Solution Approaches

10 March 2022

Dr. Johann Heyszl, Prof. Dr. Georg Sigl,
Andreas Seelos-Zankl, Dr. Matthias Hiller

Fraunhofer Institute for Applied and Integrated Security AISEC, Germany

https://data.europa.eu/doi/10.2759/640520

https://www.velektronik.de/wp-content/uploads/2023/03/Reference_paper_trustworthy_electronics_2022.pdf