Dr. Jochen Friedrich – IBM Technical Relations Europe
jochen@de.ibm.com

Cyber Security – Begriffsklärung und wachsende Bedeutung

Pushing Eastern Europe Forward - Part V

Online Konferenz | 12. Oktober 2021

Cybersecurity – Digital Security

Digital security is essential for trust in the digital age.

Why “digital security” instead of “cybersecurity”?

Digital security refers to the economic and social aspects of cybersecurity, as opposed to purely technical aspects and those related to criminal law enforcement or national and international security. The term “digital” is consistent with expressions such as digital economy, digital transformation and digital technologies. It forms a basis for constructive international dialogue between stakeholders seeking to foster trust and maximise opportunities from ICTs.

Source: OECD – https://www.oecd.org/sti/ieconomy/digital-security/

Security Operations – Mange the Risks

The acceleration in digital transformation has, over the past 12 months, affected organizational relationships with IT. Increases in remote work, use of mobile devices and cloud services have been notable, and they have facilitated a significant change in the way businesses need to function. Changes have brought about a shift in the types of threats that organizations are subject to and there is an emerging need to increase visibility to previously unmonitored third-party systems and services. […] Security and risk management leaders are unable to prepare for every eventuality and, therefore, must make intelligent, business-driven decisions about which security operations technologies they choose to manage the risks to their organization.

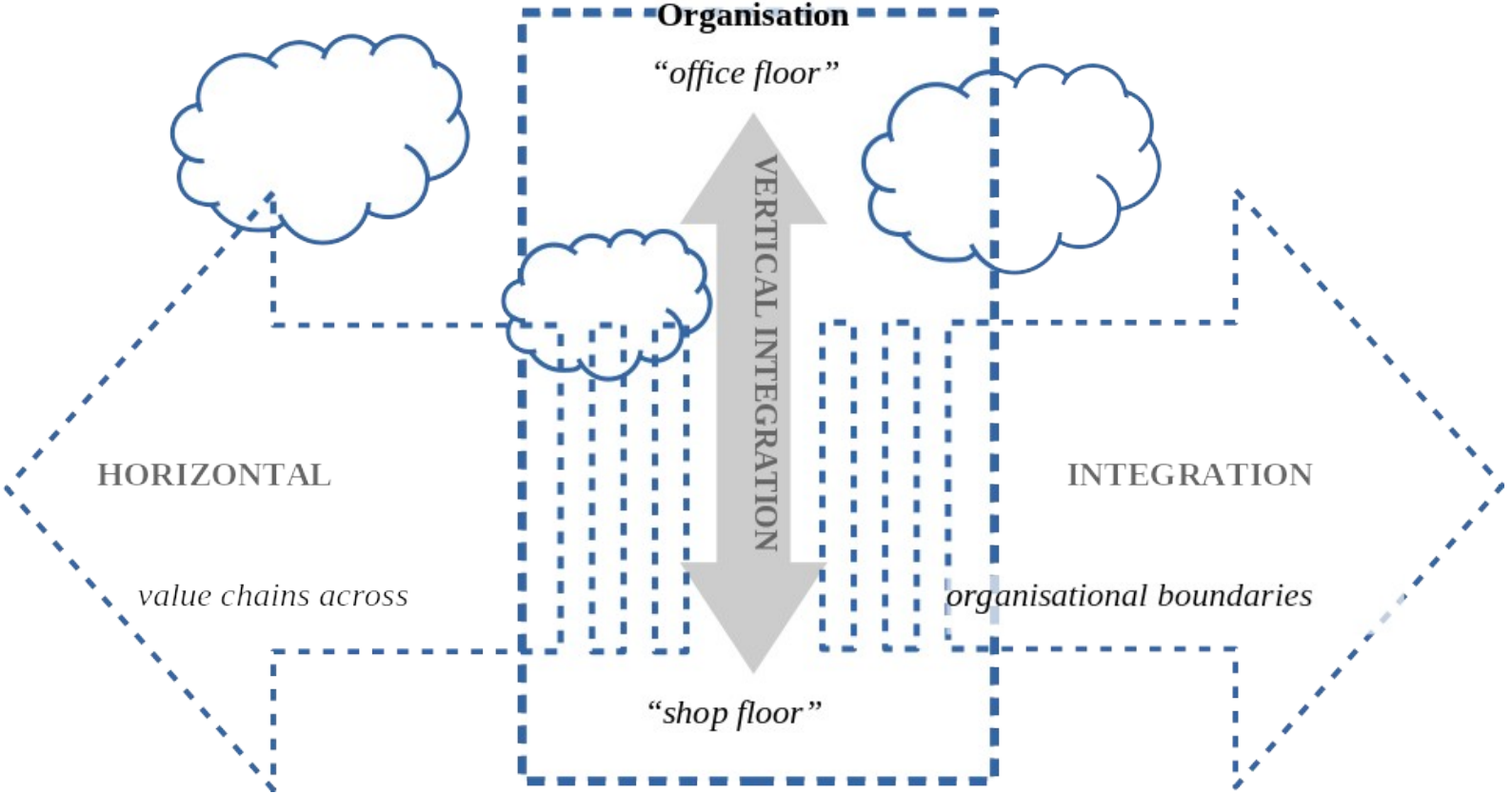
The demands of security are still heavily weighted in favor of effective processes and skilled individuals, with technologies becoming an enabler or efficiency-driver for an already effective SecOps team.

Source: Gartner Hype Cycle for Security Operations, 2021 –
https://cybersecurity.arcticwolf.com/Gartner-Hype-Cycle-Security-Operations-2021.html

Security is Foundational for Digitalisation

Security must be thought at all levels – from basic building blocks to service and application layers

And within an open collaboration framework



Standards for Cybersecurity

Standards provide a basis for ensuring high levels of security and an adequate risk-based approach

“Most modern information security and risk management standards therefore call for a risk-based approach to the selection of appropriate security controls.”

Source: ENISA Methodology for Sectoral Cybersecurity Assessments (September 2021)

Security vs. Safety

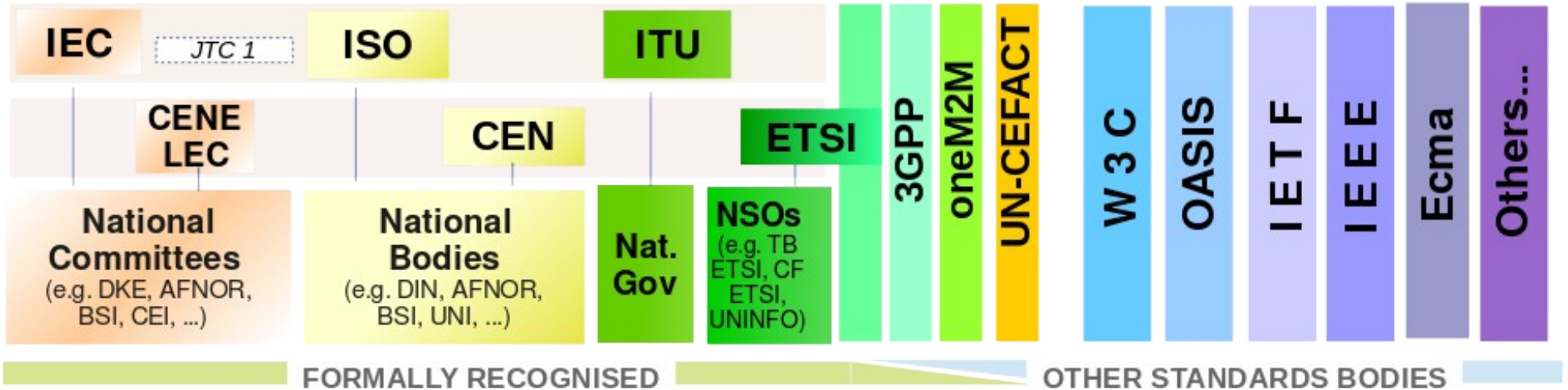
SECURITY

ISO/IEC JTC 1 SC 27
ISO 27000 series
ISO 15408

IEC Standards, in particular
IEC 61508,
IEC 61511,
IEC 62443

SAFETY

Leading Standardisation Work – Examples



IEC TC 65

ISO/IEC JTC 1SC 27

CEN-CENELEC JTC 13

DIN KITS & NIA 27

ITU-T SG 17 …

ETSI TC Cyber

W3C WebAppSec Cryptography …

OASIS CTI CSAF …

IETF I2NSF MILE …

IEEE P1912 MACSec …

Ecma Secure EcmaScript …

Complementing Standardisation

Developed in close collaboration between the Cloud Select Industry Group and the European data protection regulatory bodies

Aligned with GDPR

Ten key principles for best possible cybersecurity and privacy

Self-commitment of industry

Charter of Trust

Security by Default

Risk-based approach

Covering full supply chain

17 Baseline Requirements

Mapping to International Standards

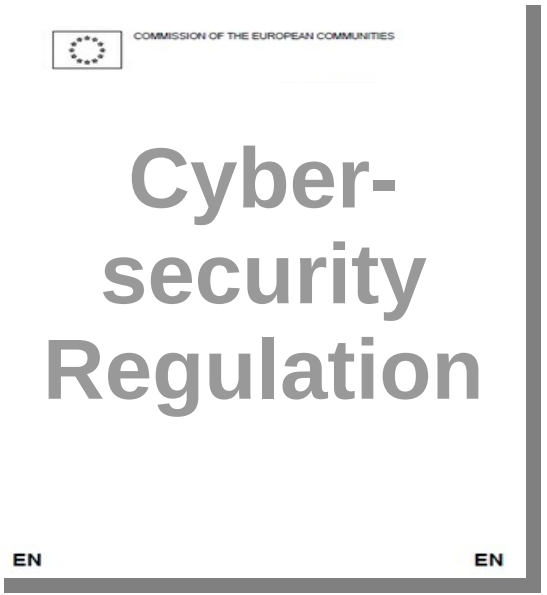
Category	Baseline Cybersecurity Supply Chain Requirements
Data Protection	Products or services shall be designed to provide confidentiality, authenticity, integrity and availability of data
	Data shall be protected from unauthorized access throughout the data lifecycle
	The design of products and services shall incorporate security as well as privacy where applicable
Security Policies	Security policies consistent with industry best practices such as ISO 27001, ISO 20243, SOC2, IEC 62443 shall be in effect
	Guidelines on secure configuration, operation and usage of products or services shall be available to customers
	Policies and procedures shall be implemented so as not to consent to include back doors, malware, and malicious code in products and services.
Incident Response	For confirmed incidents, timely security incident response for products and services shall be provided to customers
Site Security	Measures to prevent unauthorized physical access throughout sites shall be in place
Access, Intervention, Transfer & Separation	Encryption and key management mechanisms shall be available, when appropriate, to protect data
	Appropriate level of identity and access control and monitoring, including third parties, shall be in place and enforced
Integrity and Availability	Regular security scanning, testing and remediation of products, services, and underlying infrastructure shall be performed
	Asset Management, Vulnerability Management, and Change Management policies shall be implemented that are capable of mitigating risks to service environments
	Business continuity and disaster recovery procedures shall be in place and shall incorporate security during disruption, where applicable
	A process shall be in place to ensure that products and services are authentic and identifiable
Support	The timeframe of support, specifying the intended supported lifetime of the products, services or solutions shall be defined and made available
	Based on risk, and during the timeframe of support, processes shall be in place for: (1) Contacting Support, (2) Security Advisories, (3) Vulnerability Management, and (4) Cybersecurity related Patch Delivery and Support
Training	A minimum level of security education and training for employees shall be regularly deployed (e.g., by training, certifications, awareness)

Trusted Environments

objective	create an open, transparent and secure digital ecosystem, where data and services can be made available, collated and shared in an environment of trust
ecosystem	data ecosystem, the infrastructure ecosystem, and the federation services common rules (Policies and Rules) and guidelines for the consistent use of standards (Architecture of Standards) form the basis of the system

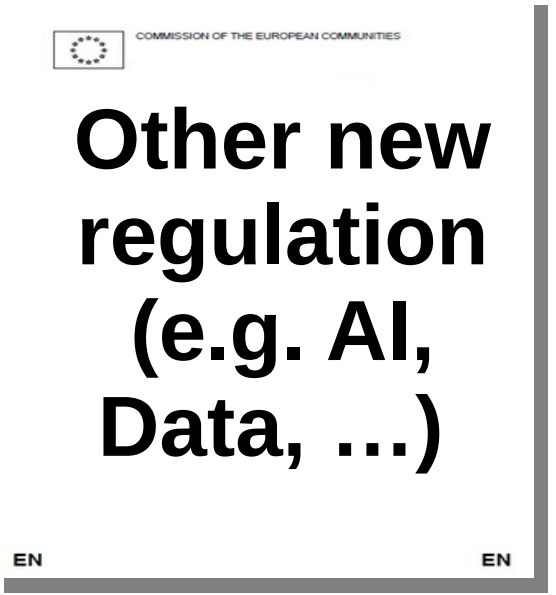
“New” regulated areas: Security and Privacy

“New” regulated areas: Security and Privacy



Draft under preparation

Delegated Act to include Cybersecurity



Compliance with EU Regulation

EU New Legislative Framework (NLF) – based on "New Approach"

European Legislators

REGULATION/ DIRECTIVE

⟺

Industry and other stakeholders

STANDARDS

Regulatory requirements

Areas: Health, Safety, Environment, Public Interest

EU Regulation
(Immediately valid throughout EU)

EU Directive → Transposition into **national law**

Standards

Industry and other stakeholders

Voluntary development of standards that meet regulatory requirements (including adoption of International Standards for Europe)

Standardisation Request (Mandate)

Conformity

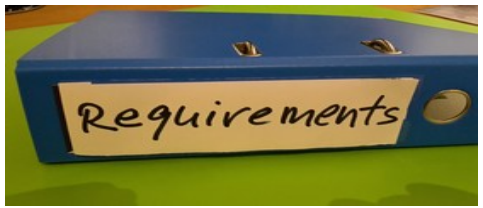
Publication in Official Journal of the EU

Test and Declaration of Conformity (SDoC)

Presumption of Conformity

Standards, Compliance, Certification

REQUIREMENTS



Essential requirements which need to be met

Developed in close interaction with stakeholders

STANDARD

Methods / processes how to meet the essential requirements

Developed in SDO – open; broad consensus

CERTIFICATION

Assessment that standard is properly implemented and that requirements are met

May include self-assessment

EU Rolling Plan for ICT Standardisation

EU standardisation priorities for all sectors where ICT standards can support implementation of EU policy objectives

Requirements for standardisation and proposals for new standards developments – updated on annual level

Chapter 3.1.5: Cybersecurity

- As pdf for download –

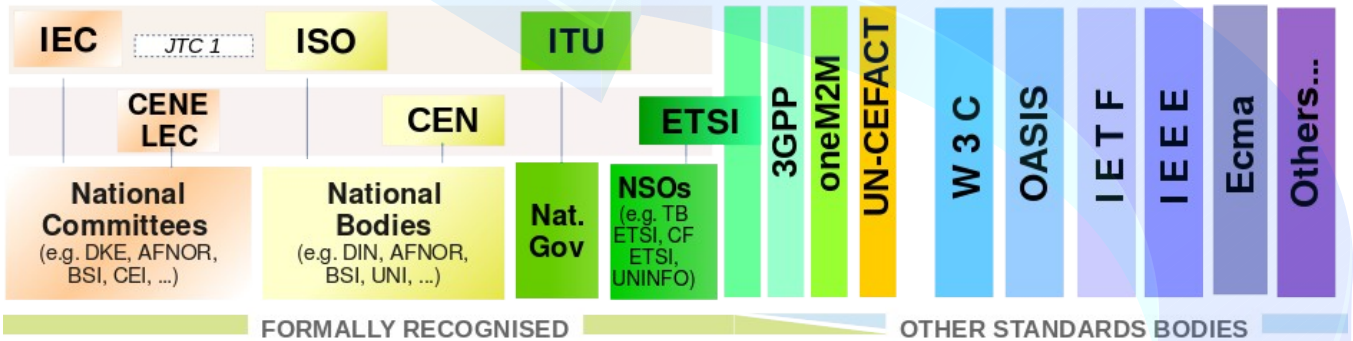
https://ec.europa.eu/growth/single-market/european-standards/ict-standardisation

- As “web version” on JOINUP –

https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/cybersecurity-network-and-information-security

Open Technology Ecosystems

standardisation



open source

Linux Foundation

Eclipse Foundation

Linux Foundation AI

Iot eclipse

node

kubernetes

Many others

Open Source Projects around Security

Some examples with IBM involvement

AI Privacy Toolkit

The AI Privacy Toolkit gives you the tools you need to assess and improve the privacy and compliance of your AI models

https://github.com/IBM/ai-privacy-toolkit/

Mesh for Data

The Mesh for Data open source project is a cloud-native platform that helps companies control and secure data usage

https://github.com/fybrik/fybrik

Universal Connector Framework

The Universal Connector Framework assists data security teams by providing a method to agentlessly collect activity and audit log data

https://github.com/IBM/universal-connectors/

Carbon for IBM Security

Carbon for IBM Security is an open source react component library built by IBM security.

https://github.com/carbon-design-system/ibm-security/

STIX Shifter

STIX Shifter connects software to products that house data repositories, ensuring data security.

https://developer.ibm.com/open/projects/stix-shifter/

API Micro Gateway

A developer-focused, programmable API gateway written in node.js to secure and control microservices and APIs.

https://developer.ibm.com/open/projects/api-microgateway/

In a Nutshell …

Cybersecurity is of foundational relevance for trust in technology and the success of the digital age.

Risk-management and risk-based approaches are at the core of successful security operations.

Standards have a key role for ensuring high levels of security and for guiding the proper approaches. Standards are complemented by Code of Conducts.

EU Regulation puts focus on security and privacy as well as on the respective standards for achieving and demonstrating compliance.

Open Source technologies complement standardisation and provide tools and technologies for improving security levels, operations and processes.

Thanks very much for your attention

Dr. Jochen Friedrich
jochen@de.ibm.com
https://www.linkedin.com/in/jochenfriedrich/
https://twitter.com/jfopen