German American Chambers of Commerce
Deutsch-Amerikanische Handelskammern

TeleTrusT Pioneers in IT security.
IT Security Association Germany

German-American IT Security Forum

IT Security Association Germany (TeleTrusT) in cooperation with GACC - German American Chamber of Commerce

San Francisco, 28.04.2025

IT Security Evaluation Landscape

Status & Needs

Marcus Krechel, TÜVIT

TÜVIT

Marcus Krechel

Head of Business Entity Evaluation & Validation

TÜVIT contact details QR-Code

tuvit.de

TÜVIT

We create trust.

IT SECURITY LAB

ACCREDITATIONS worldwilde

various SERVICES

multiple SECTORS

120+ IT Security EXPERTS

30+ years ITS EXPERIENCE

BSZ EMVCo EUCC ... FIDO NESAS TR

STANDARDS & CRITERIA

LOCATION Essen, GER

1.69 SALES in bill. EUR

>15.000 EMPLOYEES worldwide

Member of

TÜVNORDGROUP

Innovative technologies for everyone - secure, safe, sustainable & inspiring.

>500 LOCATIONS worldwide >50 countries

>150 years TIC EXPERIENCE

Status: April 2025; TNG 2024 numbers

IT Security Evaluation Landscape
Status & Needs

Agenda

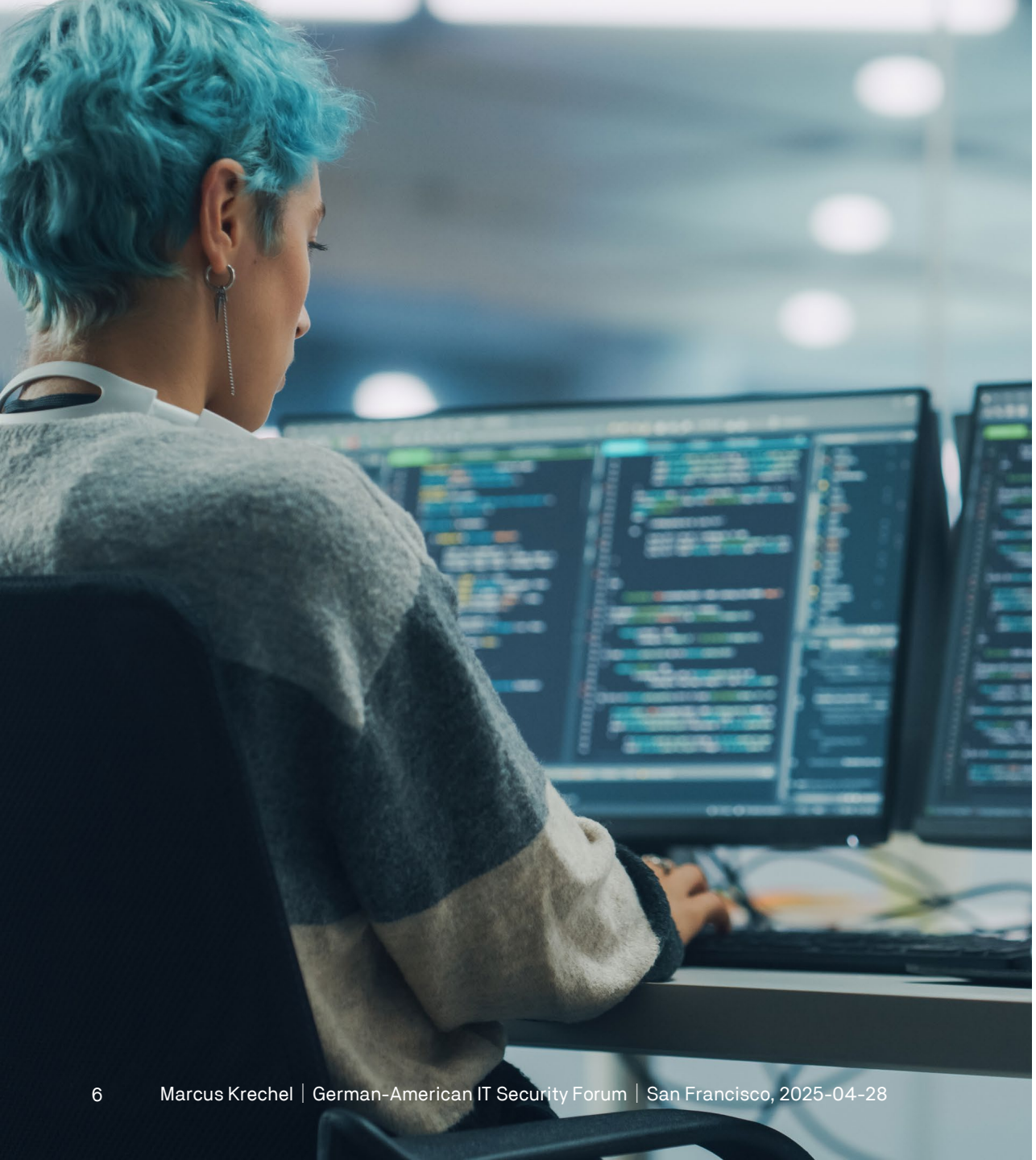
- Status
- Regulation & Certification
- Assessment Methodologies
- Challenges & Solutions
- Conclusion

TÜVIT

Status

IT Security Evaluation Landscape

- Numbers
- Vulnerabilities
- EU Cybersecurity State
- Threats Outlook



Numbers

IT Security Evaluation related April 2025

1st

Generation of EUCC labs since March 2025, incl. TÜVIT

Source: https://www.enisa.europa.eu/news

32

Years of Common Criteria evolution (start in 1993)

Source: https://www.commoncriteriaportal.org/

274.737 CVE

CVEs - until April13th 2025

Source: https://www.cve.org/

19.754 CVE

Vulnerabilities, with 9.3% critical & 21.8% high rating (2023)

Source: ENISA THREAT LANDSCAPE 2024

80 %

Number of reported incidents increased in 2023 by 80%

Source: ENISA Annual Report - Trust Services Security Incidents 2023

3.18

bill. user hours lost due to malicious actions

Source: ENISA Annual Report - Trust Services Security Incidents 2023

2.67 €

bill. € loss due to data breaches in Germany 2023

Source: ENISA THREAT LANDSCAPE 2024

2024

EUCC in place

Source: ENISA

TÜVIT

IT Security Vulnerabilities

Handling of Vulnerabilities

Common Vulnerabilities and Exposures

- Catalog for cybersecurity vulnerabilities
- Managed by MITRE; funding by DHS
- Standardised identification

Common Vulnerability Scoring System

- Standard for the severity of vulnerabilities
- Values / Categories: {0.0 .. 10.0} LOW/MEDIUM/HIGH/CRITICAL

Mandatory to use CVE database during ICT product evaluations

Some CVE examples ...

Stuxnet (CVE-2010-2772)
Exploits zero-day vulnerabilities in Windows & SCADA systems
CVSS 7.8: HIGH

Dirty COW (CVE-2016-5195)
Race Condition in the Linux kernel - Allows local users to gain root privileges
CVSS 7.0: HIGH

Spectre & Meltdown (CVE-2017/18-5715/etc.)
Processor design flaws in Intel, AMD, and ARM - Enable side-channel attacks via speculative execution, exposing system parameters
CVSS 5.6: MEDIUM

SolarWinds (CVE-2020-10148)
SolarWinds Orion API authentication bypass allows remote execution of API commands & risking system compromise
CVSS 9.8: CRITICAL

Follina (CVE-2022-30190)
Zero-day vulnerability in Microsoft Office (MSDT) exploited via manipulated Word documents
CVSS 7.8: HIGH

XZ Utils Backdoor (CVE-2024-3094)
Supply chain attack on Linux systems through manipulated xz compression library.
Goal: Remote code execution in SSH on critical systems.
CVSS 10.0: CRITICAL

2010 2014 2016 2017 2018 2019 2020 2021 2022 2023 2024

Heartbleed (CVE-2014-0160)
Security bug in the OpenSSL cryptography library, used e.g.in TLS protocol implementations
CVSS 7.5: HIGH

ShellShock (CVE-2014-6271)
Bash vulnerability on Unix based systems - Attackers can execute remote code via environment variables
CVSS 9.8: CRITICAL

EternalBlue / Wana Cry (CVE-2017-0144)
Exploit in Windows SMBv1 - Allows remote attackers to execute arbitrary code - Developed by NSA, later used for WannaCry & NotPetya
CVSS 8.8: HIGH

BlueKeep (CVE-2019-0708)
RDP vulnerability in older versions of Windows - enables "wormable" attacks without authentication
CVSS 9.8: CRITICAL

Log4Shell (CVE-2021-44228)
RCE in the widely used Java logging library Log4j. billions of devices worldwide potentially affected
CVSS 10.0: CRITICAL

Outlook vulnerability (CVE-2023-23397)
Microsoft Office Outlook Privilege Escalation Vulnerability
CVSS 9.8: CRITICAL

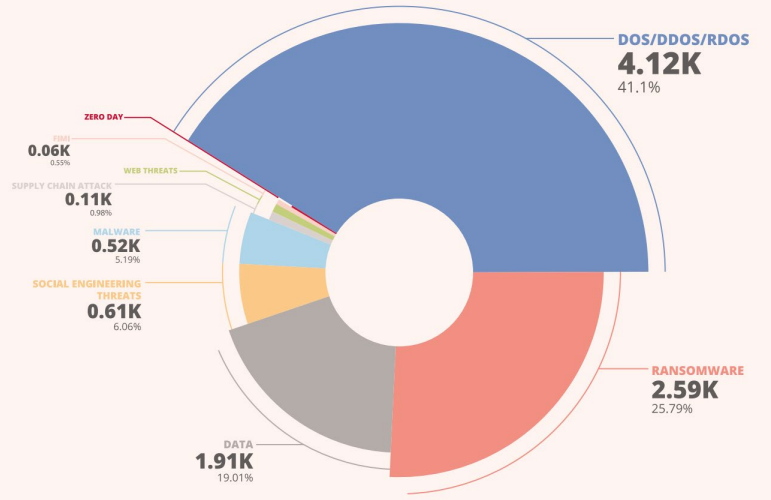
MITRE https://www.cve.org/

enisa EUROPEAN UNION VULNERABILITY DATABASE https://euvd.enisa.europa.eu/
currently in beta phase

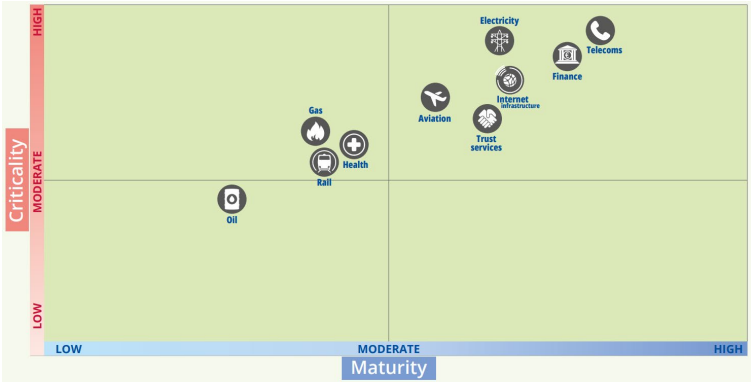
EU Cybersecurity State

ENISA Study: July 2023 to June 2024

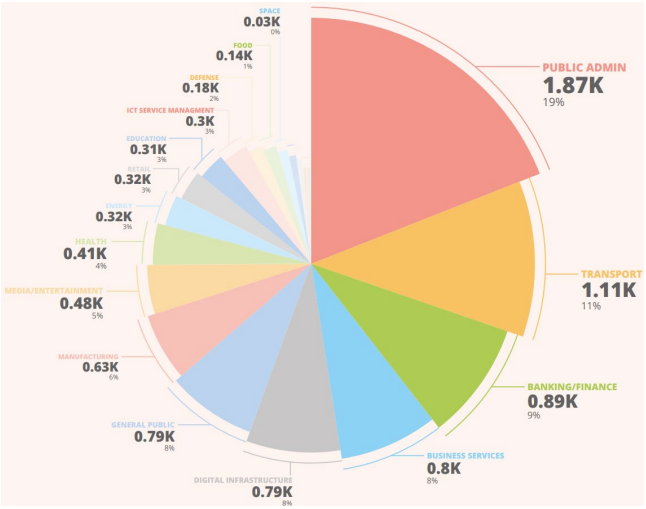
Incidents by threat type



Maturity & criticability of 10 sub-sectors



Targeted sectors per number of incidents



Source: [2024 Report on the State of the Cybersecurity in the Union.pdf]

... and more

TÜVIT

Top 11 Cybersecurity Threats for 2030

ENISA 2024

Source: 2024 Threat Landscape | ENISA

TÜVIT

Regulation & Certification

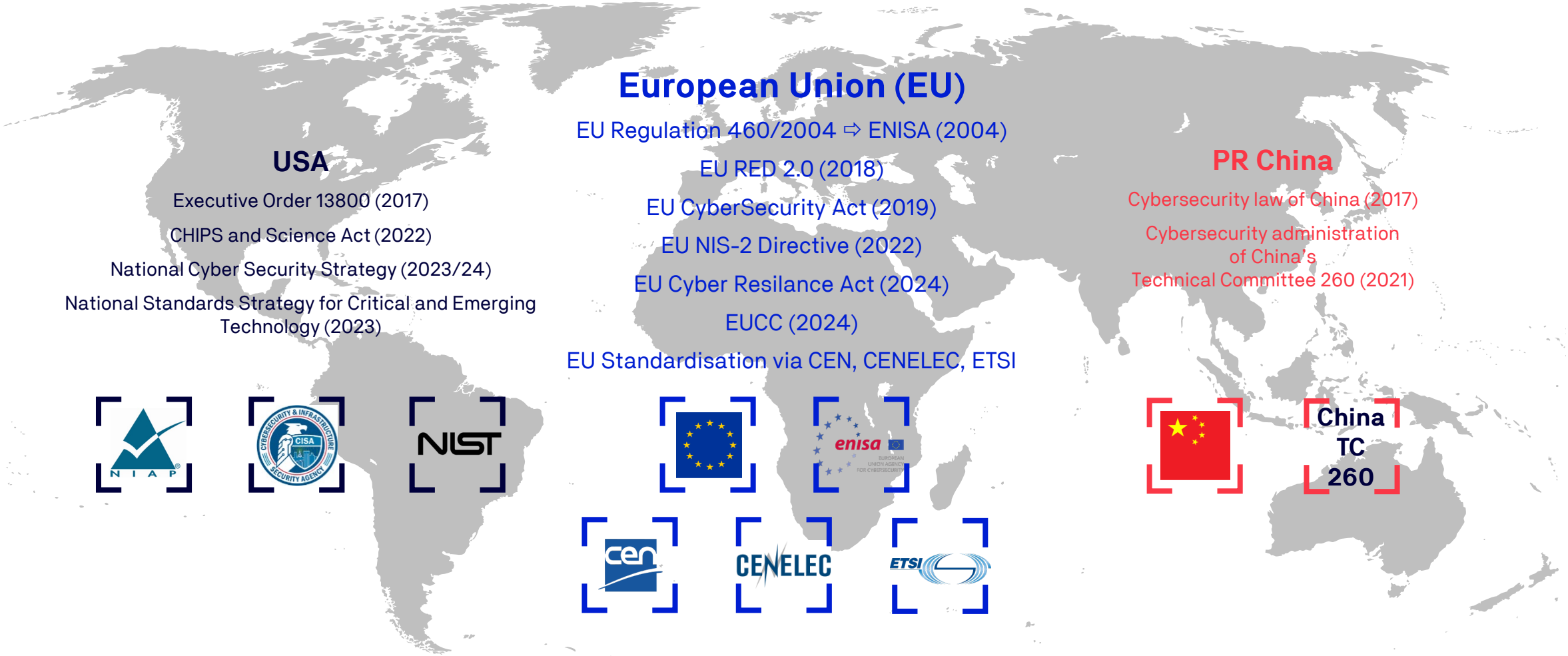
IT Security Evaluation Landscape

- Worldwide Activities
- EU CSA
- EU CRA
- EUCC

TÜVIT

IT Security Worldwide

Increased Regulation, Certification & Standardisation



USA

Executive Order 13800 (2017)

CHIPS and Science Act (2022)

National Cyber Security Strategy (2023/24)

National Standards Strategy for Critical and Emerging Technology (2023)

European Union (EU)

EU Regulation 460/2004 ⇨ ENISA (2004)

EU RED 2.0 (2018)

EU CyberSecurity Act (2019)

EU NIS-2 Directive (2022)

EU Cyber Resilance Act (2024)

EUCC (2024)

EU Standardisation via CEN, CENELEC, ETSI

PR China

Cybersecurity law of China (2017)

Cybersecurity administration of China's Technical Committee 260 (2021)

China TC 260

TÜVIT

EU Cybersecurity Act

The Underlying Framework

Purpose:

Creating a **framework** for **cybersecurity certification** across the **EU**

Strengthen EU cybersecurity

- Empowers **ENISA** (EU Agency for Cybersecurity) to manage cybersecurity at EU level
- Introduces **EU-wide cybersecurity schemes**, e.g. EUCC (2024); *EU5G/EUCS/… (i.w.)*
- **Certification assurance levels**
  - **Basic**: protection against low-skill/resources attackers
Self assessment; limited checks
  - **Substantial**: protection against skilled attackers with moderate resources
3rd party assessment (CAB)
  - **High**: protection against sophisticated attackers with significant resources
Certification (NCCA)
e.g. for critical infrastructure, government IT, 5G core networks products

TÜVIT

EU Cyber Resilance Act

Secure ICT Products Enforcement

Purpose:

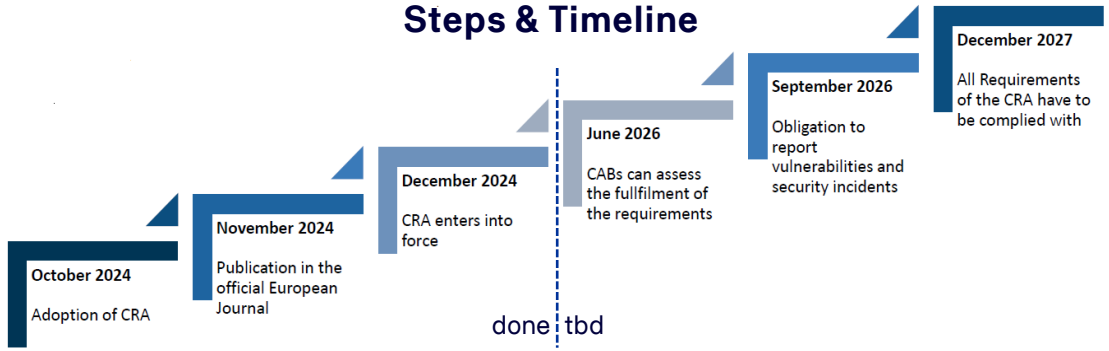
Making **cybersecurity legally mandatory for ICT products** in the **EU**

Ensuring that **ICT products** are **secure** throughout their **lifecycle**

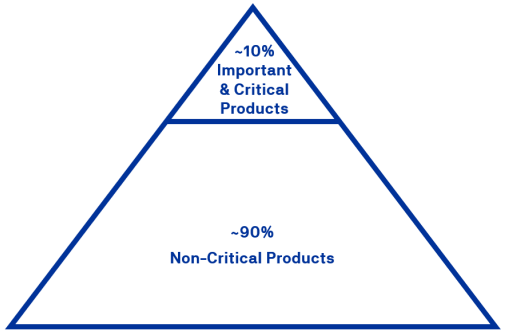
Obligations for manufactures

- Ensuring Security-by-Design & Security-by-Default
- Risk assessment before market release
- Timely security updates throughout product lifecycle
- Vulnerability handling

Steps & Timeline



ICT product distribution



Penalties

up to 15 M.€ or 2.5% of annual global turnover

Product Categories & Conformance

TÜVIT

EU Cyber Resillance Act

Product Categories & Conformance

Product Category	Default „Unclassified“	Important Class I	Important Class II	Critical
Conformance	**Self-Assessment** acc. to hEN one Module of A or B+C or H	**Self-Assessment** acc. to hEN or **3rd Party Conformity Assessment**	**3rd Party Conformity Assessment** one Module of B+C or H	**Certification** acc. CSA scheme (e.g. with EUCC)
Examples	Smart Speakers Photo Editing Software Hard Drives Mobile and Desktop Apps Games etc.	Browser Password Managers Boot managers PKI Software OS Router/Modem/Switch Microprocessor Smart Home Assistants Wearables etc.	Hypervisors & Container Runtimes Firewalls Intrusion Detection Systems Tamper-resistant MCU etc.	Smart Meter Gateways Smart Cards or similar Hardware Devices with Security Boxes Secure Elements HSM etc.

TÜVIT

EUCC

Overview

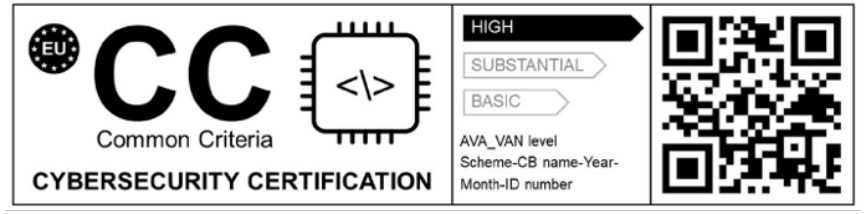
European Cybersecurity Certification Scheme on Common Criteria (EUCC)

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Common Criteria

for Information Technology Security Evaluation

ISO 15408



EUCC product certification label

- First scheme under EU CSA
- **EU harmonized certification of ICT products**
- Replaces & unifies national schemes under a single EU-level framework
- EU-wide recognition
- CC scope: product-level evaluation; coverage of product design, implementation, testing & lifecycle
- **Certification assurance levels**
  - **Basic**: n/a
  - **Substantial**: private CAB as CB, with private ITSEF (AVA_VAN.1/2)
  - **High**: public CAB as CB, with private ITSEF (AVA_VAN.3/4/5)
- **Vulnerability reporting & security updates along the product lifecycle**
- Monitoring of certified products
- Mandatory in EU since FEB 27th 2025

TÜVIT

Assessment Methodologies

IT Security Evaluation Landscape

- Overview
- Categorisation

TÜVIT

Assessment Methodologies

Overview

Common Criteria

ISO 15408

EUCC

CCRA

fixed time FiTCEM

BSPA **BSZ** **CSPN** **LINCE**

CYBERSECURITY LABEL

NCSC **BSI** **CSA**

TEE **Global Platform™** **SESIP**

ioXt internet of secure things · psacertified™ · matter

MOBILE COMUNICATION

GSMA NESAS

NESAS CSS-GI

GSMA eUICC (eSA)

APP Defense Alliance

AUTOMOTIVE

CPOC
Collaborative Intelligent Transport Systems (C-ITS) POC

PAYMENT

EMVCo

Common.SECC

Payment Card Industry

TRANSPORT

Calypso Networks Association **Calypso**

FeliCa

MIFare

CRYPTO

FIPS PUB 140-3
Federal Information Processing Standard Publication 140-3

ID & DIGITAL SIGNATURE

eIDAS
Electronic Identification, Authentication and Trust Services

ACCESS CONTROL

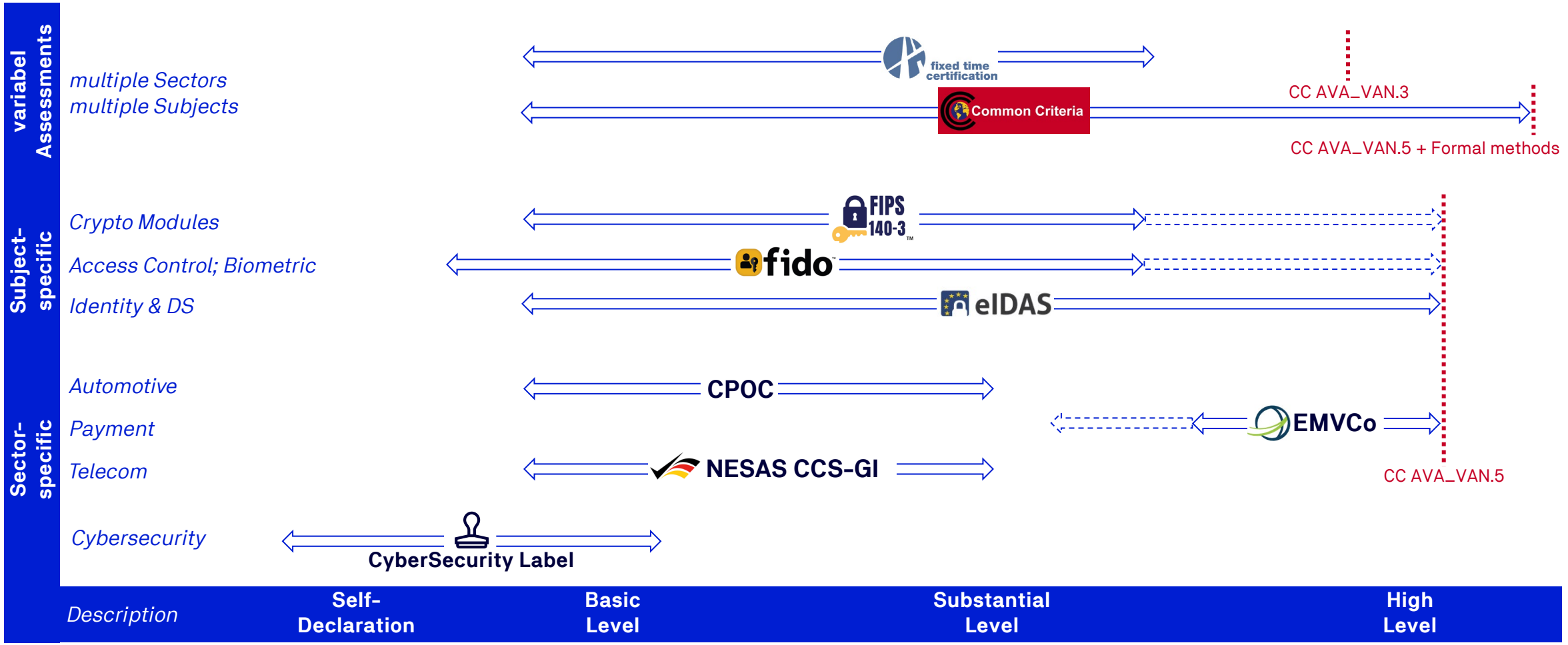
FIDO incl. Biometrics

ISO 62443

Source: based on ENISA 2024 Cybersecurity Assessments & TÜVIT

Assessment Methodologies

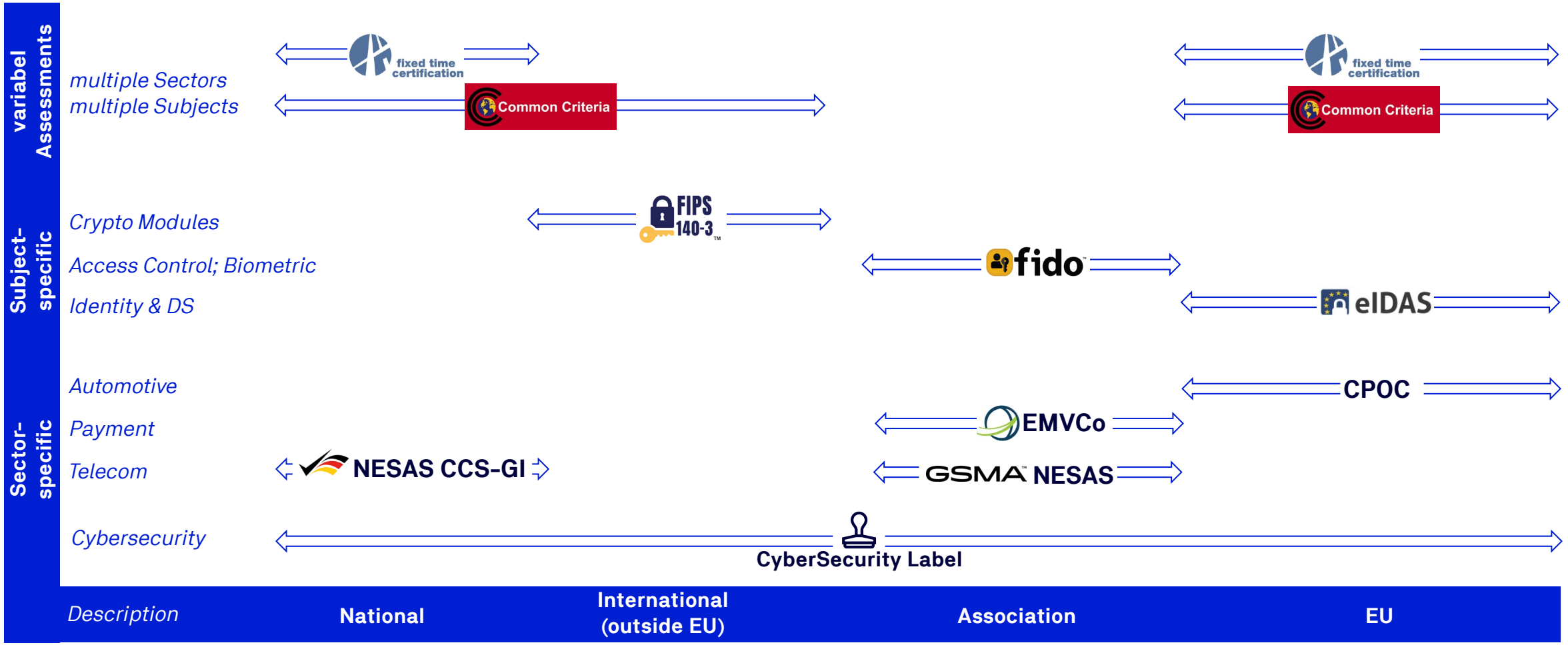
Categorisation & Leveling *informal



TÜVIT

Assessment Methodologies

Operation Sakeholder by Region



TÜVIT

Challenges & Solutions

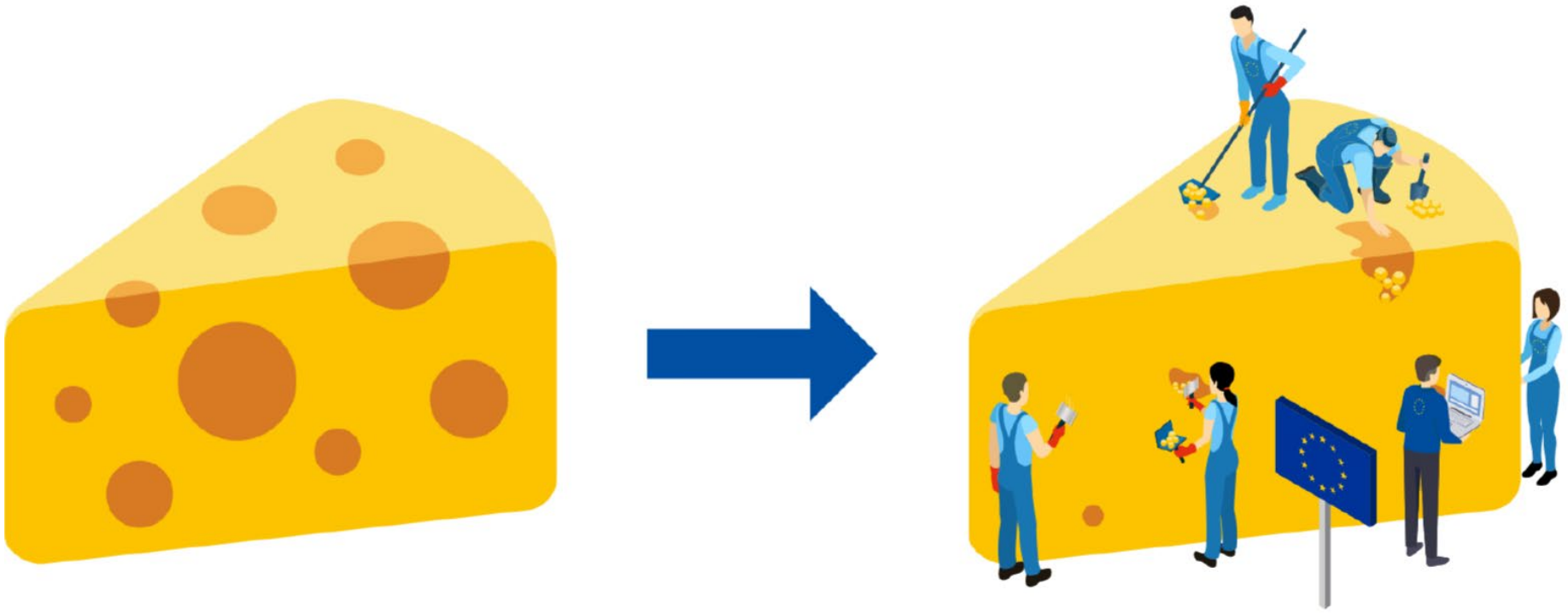
IT Security Evaluation Landscape

- EU CRA in a „nutshell“
- EUCC / CCRA Certification Recognition
- Sector Coverage

TÜVIT

EU CRA

In a „nutshell“



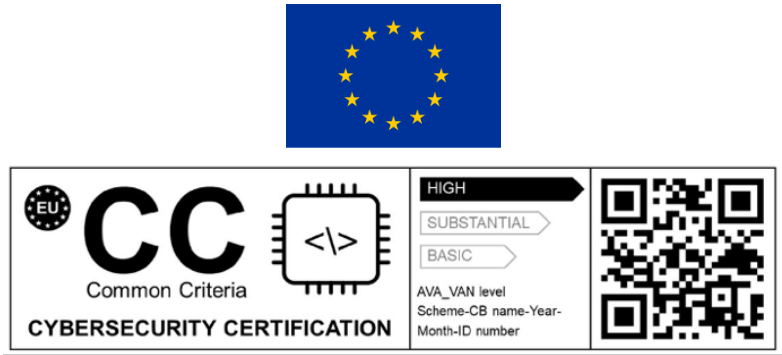
Source: EU CRA presentation; EC, CNECT.H2, DG CONNECT (2025)

European Commission

TÜVIT

EUCC & CCRA

Mutual Certification Recognition



EUCC Crtificate

Common Criteria Recognition Arragement (CCRA)

International agreement among 30+ countries (EU+international) ensures mutual recognition of certification

EU-wide EUCC certificate recognition?

Yes

EUCC & CCRA certificates - Are they mutually recognized?

No (not yet)

EUCC ≠ CCRA

(different governance, recognition, and legal frameworks)

TÜVIT

Standardisation, Certification & Sector coverage

Example: IT Security for Space

tbd

Conclusion

IT Security Evaluation Landscape - Status & Needs

TÜVIT

IT Security Evaluation Landscape - Status and Needs

Conclusion

Challenges

- Only one EU certification scheme in place (EUCC)
- Critical sectors need IT Security evaluation push (e.g. EU5G, Space)
- Flexible handling of changing threat landscape

Solutions

- EU CSA & EU CRA as trustworthy & security-driven ecosystem
- New approach includes a continuous vulnerability reporting & product update enforcement
- New concept with more private sector responsibility and more obligations

Statements

- IT Security evaluation is a dynamic & ongoing journey
- State-of-the-art standardisation is important
- Harmonised regulation & comparability are required

“Independent evaluation is an important part to increase the security of ICT products.”

TÜVIT

Thanks for your attention

Questions?

Marcus Krechel

Head of Business Entity Evaluation & Validation

E m.krechel@tuvit.de
M +49 160 888 5621
A Am TÜV 1, 45307 Essen, Germany

in https://www.linkedin.com/in/marcus-krechel-5024949/

TÜVIT contact details QR-code

LinkedIn QR-Code