Cybersecurity Compliance Connected Devices

23.10.2024

IOT & RADIO EQUIPMENT DIRECTIVE

BUREAU VERITAS

SPEAKER

MICHAEL BEINE

Business Unit Manager
Cyber Security

+49 2102 749 405
michael.beine@bureauveritas.com

BUREAU VERITAS

SUMMARY

01.
Overview

HOLISTIC VIEW ON CYBER SECURITY

PEOPLE

- Security awareness
- Training & E-Learning
- Phishing Tests
- Red Teaming
- Developer Training

PROCESS

- Security Maturity Review
- NIS Directive compliance
- Tabletop crisis simulation
- IT/OT risk & site assessment
- IT/OT governance (strategies, policies, incident response)
- Vendor Assessment

TECHNOLOGY

- Threat modeling
- IT/OT vulnerability assessments & penetration testing
- Design/capabilities review, configuration review, code review
- Product certification (IEC 62443, Common Criteria, Radio Directive)

Bureau Veritas
Cybersecurity Service Portfolio

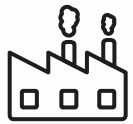
BUREAU VERITAS CPS CYBERSECURITY MARKETS

IoT

Driven by RED and CRA regulation

Based on ETSI EN 303 645 standard

Many products assessed
Authorization as Notified Body @ BV-LCIE
Accreditation as ISO17025 Testlab @ BV-7layers



Industrial

Driven by Market and NIS2 regulation

Based on IEC 62443 standard

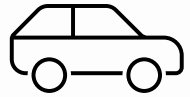
CB @ IECEE & ISA-Secure Market Leader for IECEE certification (>50% of certif.)

Medical Devices

Driven by MDR and FDA regulation

Based on UL 2900-2 standard

ISO 17025 accr. Lab@LCIE
Several projects delivered.



Automotive

Driven by UNECE R155/156 regulation

Based on ISO 21434 standard

TS Recognition at E49, E4 & E5
Accreditation for ISO 21434

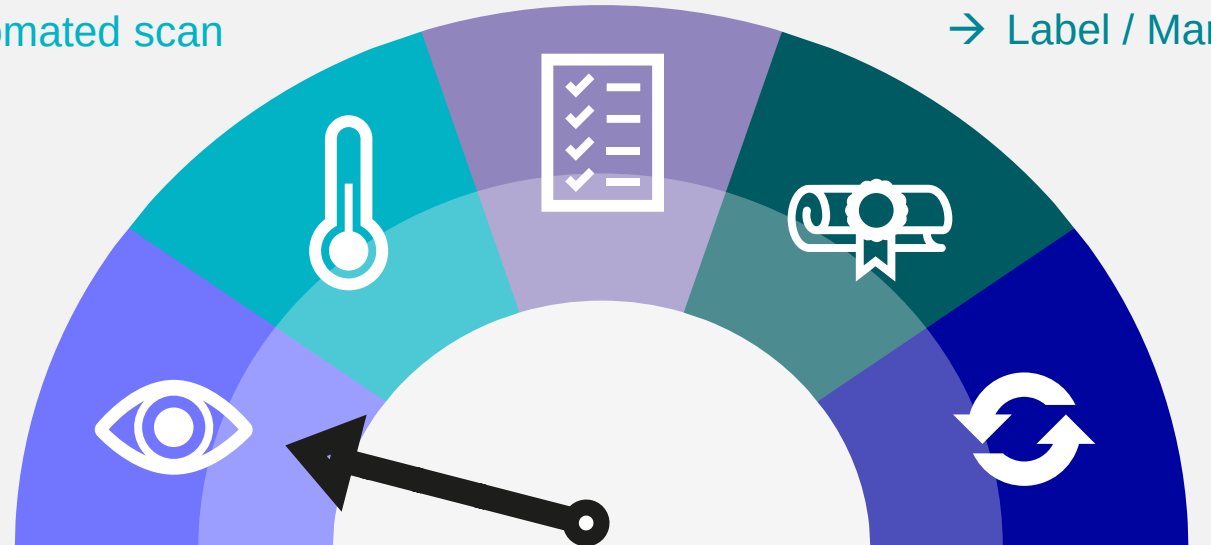
02.
Cybersecurity Compliance

CYBERSECURITY COMPLIANCE JOURNEY

Awareness
create and improve awareness about cyber security and compliance at decision making level
→ Webinar
→ Deep Dive
→ Risk Analysis

Health Check
low-level entry point to easily get a first impression of potential vulnerabilities and a high-level impression of readiness / gaps
→ Black box automated scan

Assessment
extend to a full coverage.
gather additional compliance evidence
→ Guided vendor questionnaire
→ Testing

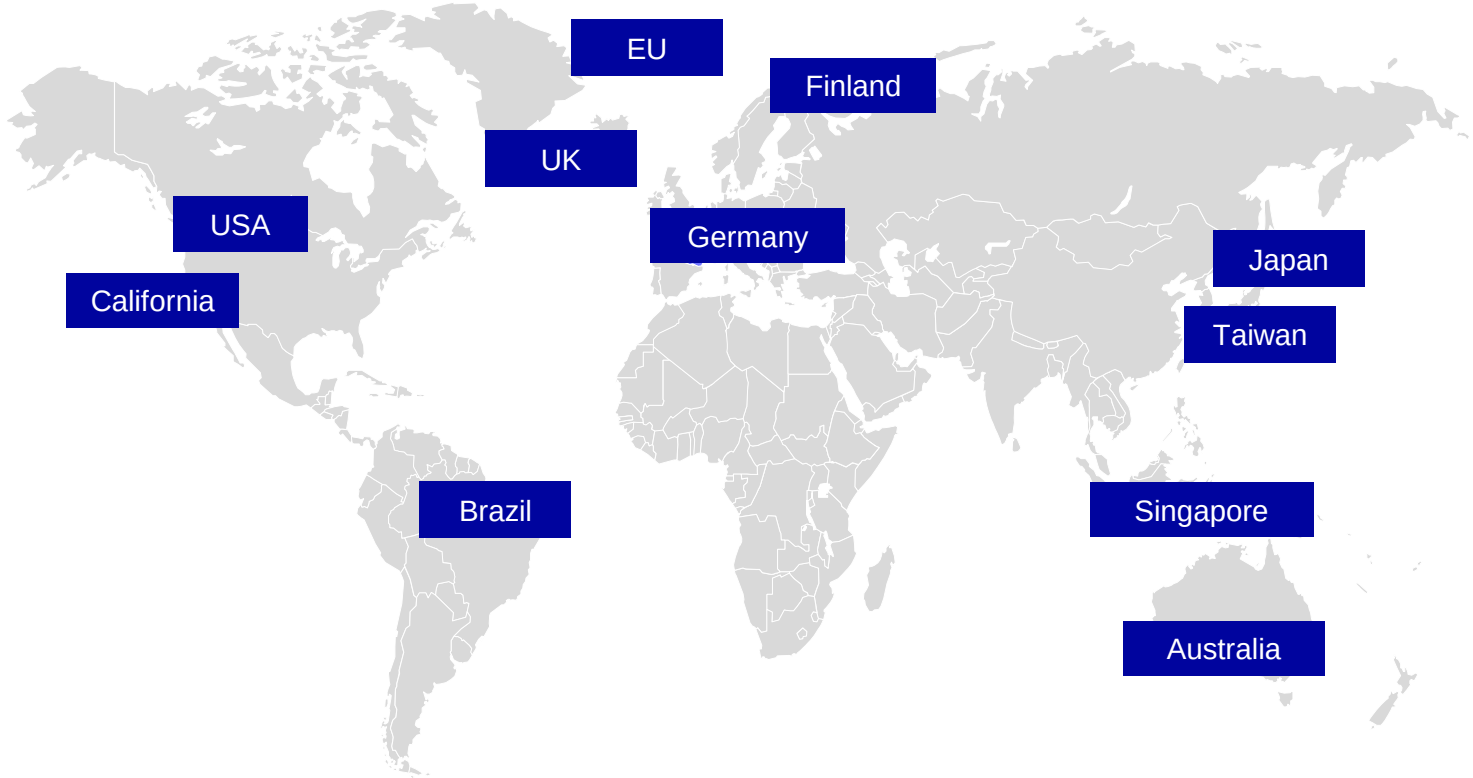


Certification
enable actors to demonstrate compliance to regulators and show security level to the market
→ Compliance docs
→ Certificate
→ Label / Mark

Update
address the full life cycle of products including updates
→ Vulnerability monitoring
→ Compliance monitoring

03.
Cybersecurity Regulations

LANDSCAPE OF CYBERSECURITY REGULATIONS



IoT Cyber Trust Mark

SB327

ANATEL ACT 77

Tel Business LAW ART 34-10

NCC Embedded Smartphone SW

CLS

Consumer IOT Regulation / Label

UK-PSTI

RED, CSA, CRA

IT-Sicherheitskennzeichen

Traficom Consumer IoT Label

04.

UK - PSTI

UK – PSTI (PRODUCT SECURITY AND TELECOMMUNICATION INFRASTRUCTURE)

- Scope: Relevant connectable products made available to consumers in the United Kingdom
- "internet-connectable products" OR "network-connectable products"
- **Applicability Date: 2024-04-29**
- Compliance: Manufacturer to ensure that a Statement of Conformity (SoC) accompanies the product when making it available.
- Importer and Distributer in UK are also held responsible for compliance.

Office for Product Safety & Standards

UK – PSTI (PRODUCT SECURITY AND TELECOMMUNICATION INFRASTRUCTURE)

REQUIREMENTS MAPPING TO ETSI EN 303 645:

"Passwords" --> provision 5.1-1 AND 5.1-2

- "Information on how to report security issues" --> provision 5.2-1
- "Information on minimum security update periods" --> provision 5.3-13

Link: https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime

BV-Service:
- 3rd Party Assessment
- white label SoC

05.

EU - RED

EU – RADIO EQUIPMENT DIRECTIVE (RED)

- Scope: Delegated Regulation DR(EU)2022/30 was published in Official Journal (EUOJ) on 2022-01-12
- Applies to Radio Equipment, which can be connected to the Internet.
- Exceptions: Already covered by other EU regulation like Medical, Automotive, Smart Meter, eIDAS
- Applicability Date: Aug **2025 → when products are place on th**e market (including legacy products)
- Compliance: EU Type Examination Certificate by Notified Body **OR**
  Declaration of Conformity based on Self-Assessment (after release of harmonized Standard)

BV-Service:
- Preparation & Risk Analysis
- 3rd Party Assessment based on applicable Standards
- EU Type Examination Certificate by Notified Body

EU – RADIO EQUIPMENT DIRECTIVE (RED)

REQUIREMENTS

- Article 3.3.d: radio equipment does **not harm the network** or its functioning nor misuse network resources,
  thereby causing an unacceptable degradation of service.
- Article 3.3.e: radio equipment incorporates safeguards to ensure that the **personal data and privacy** of the user and of the subscriber are protected.
- Article 3.3.f: radio equipment supports certain features ensuring **protection from [monetary] fraud.**

Standards: ETSI EN 303 645+Delta, IEC 62443+Delta, CEN/CENELEC 18031 (candidate for hEN)

Link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:007:FULL&from=EN

EU – CYBER RESILIANCE ACT (CRA)

- Scope: Products with digital elements includes HW and SW
- Applicability Date: Strong positive vote in EU-parliament in March-24, Expected to be enacted by EU-council in 2024 → Enforced in 2027 (*2026)
- Scheme: CE-Mark / New Legislative Framework (NLF) + Fines & Sanctions
- Requirements:
  - Product Requirement: Security by Default, Security Updates, Access Control, Secure Data at rest and in transit, etc.
  - Process Requirements: Risk Assessment, Secure Design, Development and Production, Vulnerability Handling, etc.
  - Documentation Requirements: Support Period, Vuln. Discl. Policy, Security User Guidance, *Notify about incidents, etc.

Questions:
- Roadmap + Schedule ?
- Standards and Requirements ?
- Overlap with RED ?

Link: https://ec.europa.eu/newsroom/dae/redirection/document/89543

OPTIONS TO COMPLY WITH RED-CYBER (DR (EU) 2022/30)

Requirements are Defined in EN 18031

Self-Assessment using hEN 18031

Will be possible after EN 18031 was cited in OJ as harmonized Standard by EU-Commission (??? Sept. 2024 ???)

Or

EU Type Examination issued by authorized Notified Body

- Based on Assessment using EN 18031 or
- Based on Assessment re-using EN 303 645 + Delta to EN 18031 or
- Based on Assessment re-using IEC 62443-4-2 + Delta to EN 18031

Family Approach

For a family of variant devices with same security baseline can help to reduce certification effort

BV - Benefits

EU-TEC issued by BV as NB is → "**highest possible assurance of compliance**"

Test Report issued by BV under 17025 ILAC accreditation → "**highest possible assurance of competence and quality**"

Guidance and Support in Workshops and Pilot Projects → "**BV is your companion on the compliance journey**"

06.

BV Solutions

BUREAU VERITAS - SOLUTION FOR IOT

ADDRESSING RED BASED ON ETSI EN 303 645 / TS 103 701

Step 1

Kickoff workshop to explain the requirements and prepare a Risk Analysis

As a result the manufacturer will have a good technical understanding of the cyber requirements by RED + ETSI. And guidance to establish a cyber risk analysis.

Step 2

Conceptual Assessment of Design Documentation (ICS&IXIT Questionnaire)

As a result, the manufacturer will know the current level of conformity of the design.

Can serve as **GAP-Analysis**

Step 3

Functional Assessment of the Device

As a result, the manufacturer will receive a test report confirming the level of conformity of the implementation in the device.

Step 4

Confirmation by Notified Body: EU Type Examination Certificate

As a result, the manufacturer can receive the confirmation of conformity to the RED regulation from an authorized notified body.

End to end duration typically 6-9 months

Workshop & Risk Analysis | Assessment of Design | Assessment of Device | Certification

HOW TO ADDRESS A FAMILY OF DEVICES

NO MODULAR APPROACH IN CYBER SECURITY

- Family Assumptions
  All devices belonging to the family share the same answers in Questionnaire (ICS/IXIT).
  This means they all have the same cyber security baseline.

- Family Definition
  The applicant provides a statement listing the members of the family and confirming the family assumptions.
  The applicant describes the non-cyber related differences of the members (e.g. compared to a mother device).

- Family Assurance
  Bureau Veritas performs complete assessment of one member of the family (conceptual and functional)
  Bureau Veritas selects a number of representative devices from the family
  Bureau Veritas performs spot check across representative selection of devices to verify assumption of similarity.

- Certificate Coverage
  Bureau Veritas issues a certificate of conformity to ETSI EN 303 645 listing all devices of the family.

BUREAU
VERITAS

Shaping a World of Trust