UL Solutions

Cyber Resilience Act: Implications for the Automotive Industry

24th Workshop of Automotive SPIN Italia

Fabio Bella
May 21, 2026 – Bologna, Italy

Within UL Solutions we provide a broad portfolio of offerings to many industries. This includes certification, testing, inspection, assessment, verification and consulting services. In order to protect and prevent any conflict of interest, perception of conflict of interest and protection of both our brand and our customers brands, UL Solutions has processes in place to identify and manage any potential conflicts of interest and maintain the impartiality of our conformity assessment services.

SOFTWARE INTENSIVE SYSTEMS

We deliver

Our solutions span the ESG spectrum to increase safety, security and sustainability

PEOPLE. PLANET. TRUST.

Certification

Verification

Testing

Auditing and inspection

Software

Data insights

Advisory

Learning and development

Locations and employees

Our

14,800+

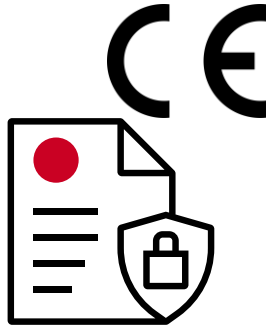
mission-driven employees work in

40+ **countries**
around the world.

Location information is as of September 2023.
Employee information is as of September 2023.

What is the EU Cyber Resilience Act (CRA)?
Key elements

- Cybersecurity requirements for **placing Products with Digital Elements** (PwDE, i.e., HW + SW + remote data processing solutions) **on the European market**
- **Different roles:** obligations for manufacturers, distributors, and importers
- Cybersecurity essential requirements **across the product life cycle**, from design, development, production, to the end of life, including mandatory risk assessments
- **Vulnerability management and incident response** to promptly identify, remediate, and report actively exploited vulnerabilities supported by continuous monitoring and reporting mechanisms



Implementation timeline

September 2026: Start reporting

December 2027: Full applicability (36 months after adoption in 2024)

Scope of CRA – Implications for Automotive Industry (1/2)

CRA does not apply to products already covered by other EU regulations

Cyber Resilience Act (CRA)

Products with digital elements

Covers Products with digital elements (HW + SW and its remote data processing solutions)

Vehicle categories*:
T, R, S, G, (+ special purpose vehicles not under M, N, L)

*T, R, S, G: alignment with ISO 24882

Excludes

General Safety Regulation (GSR) 2019/2144

Road vehicle Type approval

Covers vehicle safety, cybersecurity (via UN R155, EU national implementation with this regulation) and type approval

Vehicle categories:
M, N + ?

EU 44/2014**

technical requirements and testing procedures regarding the protection **of L-category vehicles**

→ amended via (EU) 2025/1455 against cyberattacks

+ Vehicle Category O?
+ Automotive suppliers:
(developing PwDE: developed exclusively for a specific client or internal use, not placed on the market seperately)

**Supplements (EU) No 168/2013 which is the main legislative framework for the approval and market surveillance of L-category vehicles in the EU.

Scope of CRA – Implications for Automotive Industry (2/2)
Automotive-relevant PwDE within the scope of CRA

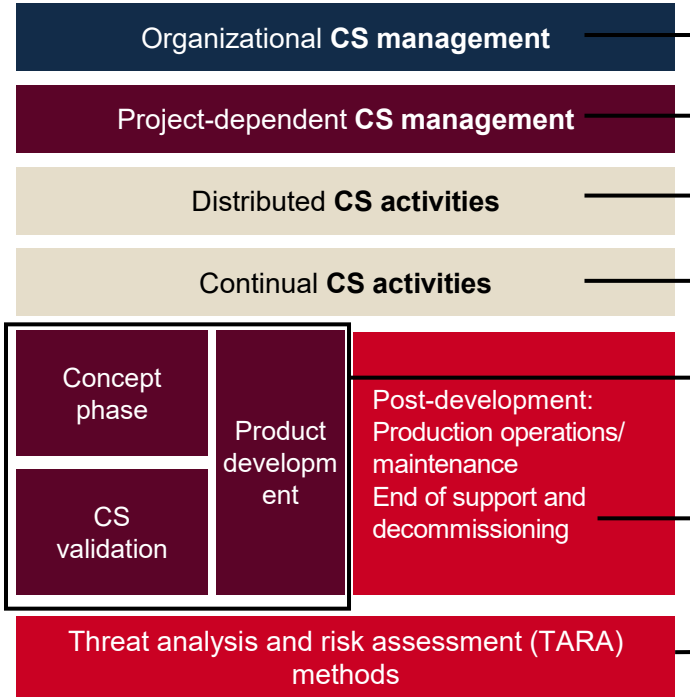
CRA applies if ANY of the following are true:

- Product is **not covered by EU type approval**
- Product is **sold independently from the automotive supply chain**
- Product is **non-onboard software** (app / cloud-based service)
- Product is **used across industries** (double regulation)

- Products outside scope of UNECE vehicle categories
  Micromobility devices (e-scooters, bikes), agricultural or construction vehicles (depending on jurisdiction specifics), certain special-purpose vehicles
- Aftermarket and non-type-approved products
  Aftermarket OBD dongles, third-party telematics devices, retrofit infotainment systems, fleet management hardware/software
- Software / services not part of vehicle type approval
  Mobile apps interacting with the vehicle, cloud backends (telematics platforms), SaaS components for vehicle data processing
- Dual-use or cross-sector products
  GNSS modules, connectivity modules (5G/LTE), IoT devices used in vehicles and elsewhere (both UNECE and CRA regulations apply)

CRA vs. ISO/SAE 21434 (1/4)

ISO/SAE 21434:2021 is a good foundation for CRA compliance



Domains of cybersecurity activities described in clauses of ISO/SAE 21434:2021

Management system supports CRA especially for module H

Supports CRA's expectations for **structured planning**

Supports CRA's **supply chain security** expectations

Supports CRA for **vulnerability mgmt**. and **monitoring** throughout the lifecycle.

Matches CRA's requirement for **security-by-design** across the entire product lifecycle

Supports CRA's requirements for production, **post-market obligations** for **security updates,** incident management and support period obligations

CRA **demands a similar risk assessment**, the method for CRA is not fixed, TARA can be used if suitable for the product

CRA vs. ISO/SAE 21434 (2/4)
Additional requirements for CRA compliance - selection

CE marking - compliance and conformity assessments

CRA mandates clear procedures for conformity assessment (Module A, B+C, H)

Software Bill of Materials (SBOM) - (indirect gap)

CRA mandates the use of an SBOM for transparency

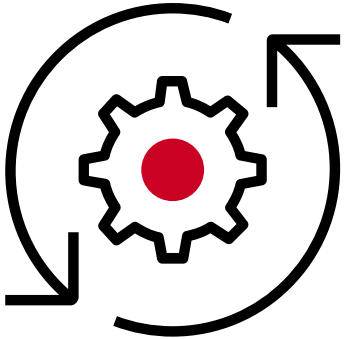
Vulnerability and Incident Management:

- CRA: notify actively exploited vulnerabilities or any severe incident to ENISA and national CSIRTs
  - early warning within **24 hours** after becoming aware
  - vulnerability/incident notification within **72 hours**, including actions to take by user
  - final report no later than **14 days** (vulnerability) or **1 month** (incident) after mitigation available
- CRA: **patches** are delivered without delay, **free of charge** and with advisory messages.

CRA vs. ISO/SAE 21434 (3/4)
Additional requirements for CRA compliance - selection

CRA mandates:

- **Support period:** shall be **no less than five years**, unless the lifetime of the product with digital elements is less than five years (effective handling of vulnerabilities!)
- **Detailed requirements for documentation:** e.g., keeping technical documentation and user manual **for at least 10 years** after the product with digital elements has been placed on the market, or for the support period, whichever is longer.
- **End date of the support period:** clearly and understandably **specified at the time of purchase** in an easily accessible manner.
- **Security updates:** shall remain available for a **minimum of 10 years** after it has been issued, or for the remainder of the support period, whichever is longer.



CRA vs. ISO/SAE 21434 (4/4)

Product categories and assessment

Category	Requirements	Module*	Examples
Default Category	Products with a lower cybersecurity risk profile require a self-assessment (technical file). Manufacturers can demonstrate compliance by conducting a self-assessment against relevant standards. → EU declaration of conformity, based exclusively on Harmonized Standards (hENs).	Module A	Memory chips, mobile apps (expected to cover 90% of PDE)
Important Class I:	If you can use a harmonized standard, you may demonstrate compliance through self-assessment. If you cannot use a harmonized standard, you must undergo a conformity assessment by a Notified Body (third-party).	Module A Optional (if A cannot be used): Module B+C Module H	Operating systems, Microprocessors/ controllers with security-related functionalities, Smart home products w. security functionality
Important Class II:	These higher-risk products always require a third-party conformity assessment by a Notified Body, regardless of harmonized standard availability.	Module B+C Optional: Module H	Firewalls, IDS, Tamper-resistant microprocessors/ controllers
Critical Category:	The highest-risk products must obtain certification under an EU cybersecurity certification scheme (such as EUCC, EUCS, or EU5G), with assurance at least at the 'substantial' level. Alternatively, if certification is not yet available, conformity assessment procedures as specified in CRA Article 32(3) apply.	Common Criteria Module B+C / Module H (Only in absence of CC)	Smart cards, secure elements, smart meter gateways

** Module: conformity assessment procedures*

Consequences in Case of Infringements

Imposition of fines

Up to €15 million or 2.5% of global annual turnover, whichever is higher. Applies to: All products with digital elements (including Default, Class I, and Class II)

Market withdrawal or distribution restrictions

Authorities may order the withdrawal of a non-compliant product from the market or restrict its distribution.

Market sweeps will detect non-compliance.

Product Recall

In serious cases, a complete withdrawal or recall of the product may be required.

Mandatory: For products posing a severe cybersecurity risk.

Details, see Article 64: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

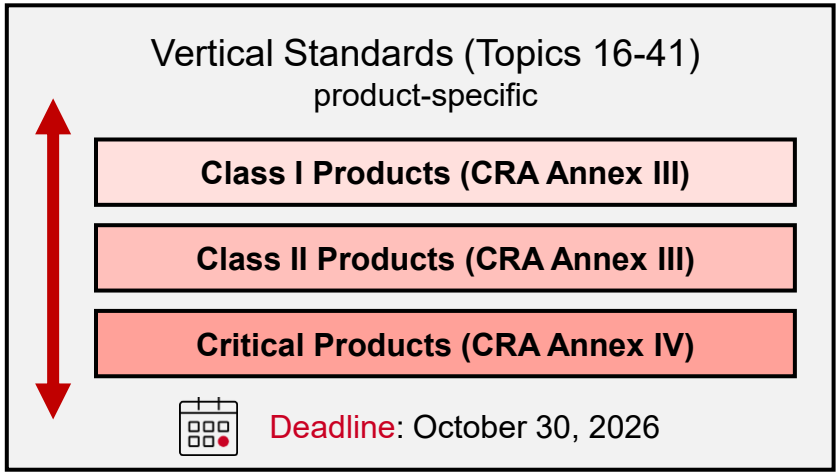
European Commission's Request for Standardization

More guidance for implementation is on its way

- The **European Commission** has requested **CEN, CENELEC and ETSI** to develop **harmonized standards** for compliance with CRA across 41 distinct topics.
- The goal is to align cybersecurity requirements across industries: IOT, Industrial, etc. as well as their supply chain such as chip vendors, and components.

CEN CENELEC ETSI
EUROPEAN STANDARDIZATION ORGANIZATIONS

Source: Cen cenelec website

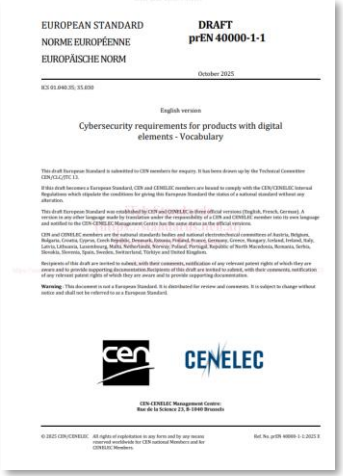


Horizontal Standards

EN 40000 Series - Cybersecurity requirements for PwDE

EN 40000-1-1 to -1-4 form a coherent horizontal framework enabling structured and demonstrable CRA compliance across all products with digital elements.

- EN 40000-1-1 Vocabulary
  Establishes a common, harmonized cybersecurity vocabulary for products with digital elements and ensures consistent interpretation of CRA requirements across manufacturers, assessors, and authorities.
- EN 40000-1-2 Principles for Cyber Resilience
  Defines core cybersecurity principles and a risk-based lifecycle approach for products with digital elements
- EN 40000-1-3 Vulnerability Handling
  Specifies mandatory processes for identifying, managing, and remediating vulnerabilities throughout the product lifecycle
- EN 40000-1-4 Generic Security Requirements
  Provides a catalogue of concrete, verifiable cybersecurity requirements for products with digital elements (based upon other standards such as EN 18031:2024 series and incorporates elements from IEC 62443-4-2 and ETSI EN 303 645)


EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

DRAFT
prEN 40000-1-1

October 2025

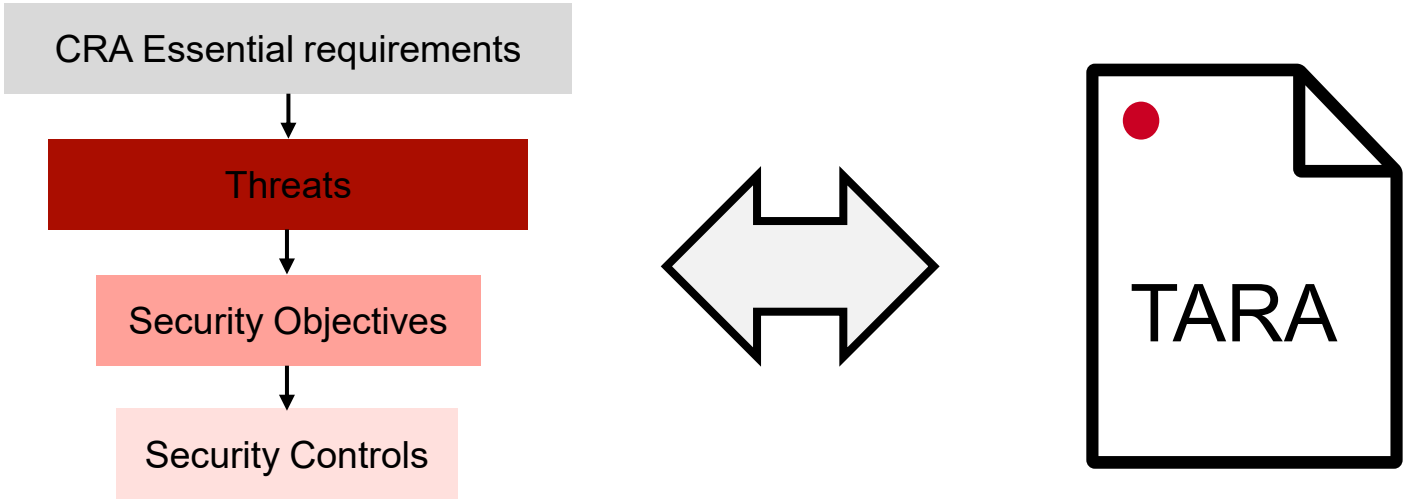
English version

Cybersecurity requirements for products with digital elements - Vocabulary

CEN CENELEC

Practical Implications – Risk Assessment

Mapping CRA security objectives and controls to TARA



Horizontal standards will specify generic cybersecurity requirements applicable for all product categories; technical reports will provide more details*:

→ a catalog of security controls with their objectives and more technical assessment criteria (building upon the EN 18031:2024 series) mapped to CRA essential requirements

*based on Cen and Cenelec webinar: Unlocking CRA Security Controls: preparation for UNE Event'

Conclusions

Is the CRA relevant for me?

Yes, if you sell connected products in the EU that are not covered by EU Regulations 2019/2144 or 44/2014

Which challenges may I face?

- The first deadline (start of reporting) is September 2026
- Limited time to wait for harmonized standards to be finalized
- Some edge cases remain unclear (e.g., Category O trailers / semi-trailers)

Which new requirements must I fulfill?

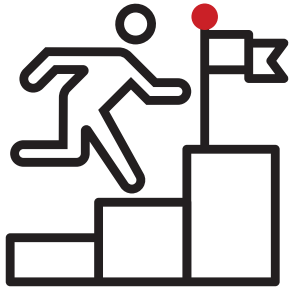
If you already comply with ISO/SAE 21434, many requirements are partially covered.

Key additional requirements include:

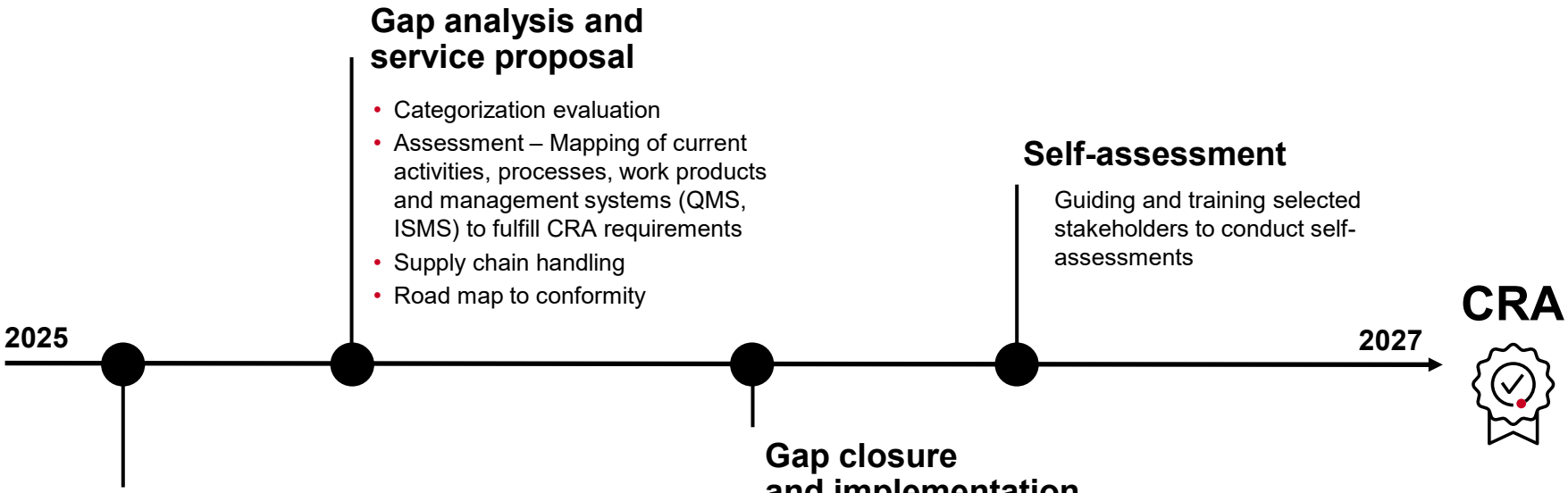
- CE marking - compliance and conformity assessments
- Software Bill of Materials (SBOM)
- Vulnerability and Incident Management
- Defined support period
- Security updates

Following Up With CRA – What Can I Do?

- ✓**Understand your CRA obligations:** determine whether your products fall within the scope of CRA → track regulatory updates
- ✓Familiarize yourself with **existing cybersecurity standards and best practices** to prepare for CRA compliance even before the harmonized standards are officially published
- ✓**Integrate with existing cybersecurity frameworks**: align cybersecurity processes and methods with ISO 21434 and map CRA requirements → smart integration into CSMS
- ✓**Be part of the working groups** and actively shape harmonized standards towards your needs



UL Solutions Service Approach



Introduction

- Key stakeholder or decision-maker – Half-day intro session
- Selected stakeholders and process owners – Two-day training sessions

Gap analysis and service proposal

- Categorization evaluation
- Assessment – Mapping of current activities, processes, work products and management systems (QMS, ISMS) to fulfill CRA requirements
- Supply chain handling
- Road map to conformity

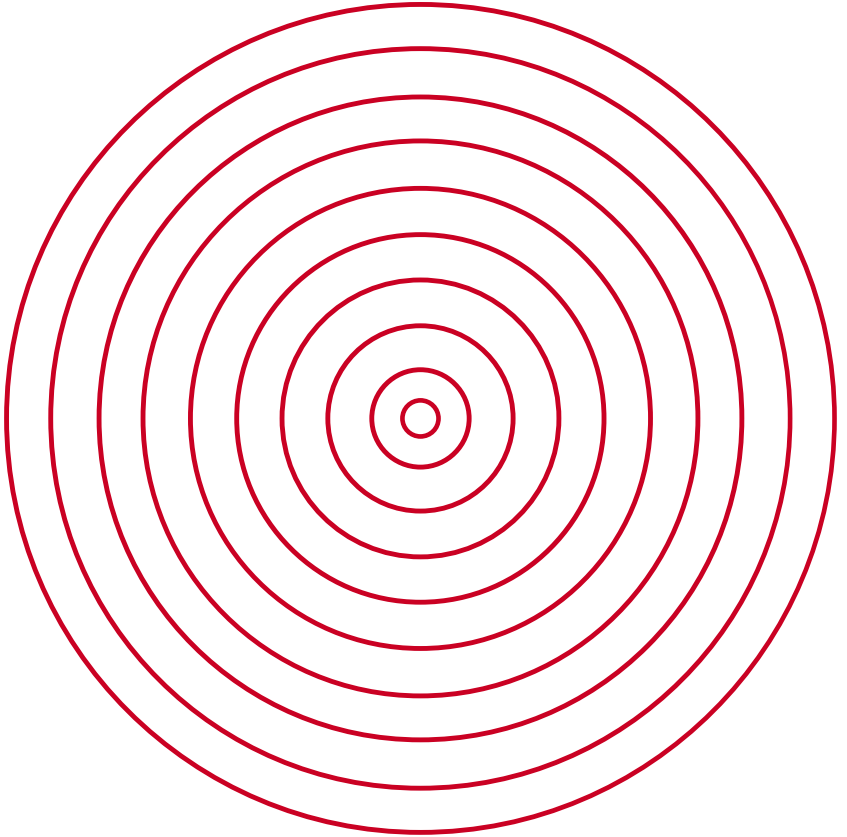
Gap closure and implementation

- Apply improved organizational processes to integrate CRA requirements into daily operations, enabling consistent and sustainable compliance with CRA requirements
- Duration – Minimum 12 weeks, maximum 40 weeks

Self-assessment

Guiding and training selected stakeholders to conduct self-assessments

Questions?



Fabio Bella
Fabio.Bella@UL.com

UL.com/Solutions

Thank you

UL.com/SIS

Within UL Solutions we provide a broad portfolio of offerings to many industries. This includes certification, testing, inspection, assessment, verification and consulting services. In order to protect and prevent any conflict of interest, perception of conflict of interest and protection of both our brand and our customers brands, UL Solutions has processes in place to identify and manage any potential conflicts of interest and maintain the impartiality of our conformity assessment services.

References

Main References

- EU Cyber Resilience Act (Regulation EU 2024/2847)
- Cyber Resilience Act implementation - Frequently asked questions | Shaping Europe's digital future
- ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering
- UN Regulation No. 155 - Cyber security and cyber security management system
- EN 40000 Series - Cybersecurity requirements for products with digital elements
  - EN 40000-1-1 Vocabulary
  - EN 40000-1-2 Principles, product risk management, and lifecycle activities
  - EN 40000-1-3 Vulnerability Handling
  - EN 40000-1-4 Generic Security Requirements

Basis for EN 40000 Series

- EN18031:2024 Series - Common security requirements for radio equipment
  - Part 1: Internet connected radio equipment
  - Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment
  - Part 3: Internet connected radio equipment processing virtual money or monetary value
- IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components
- ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements

Vulnerability Disclosure & Handling

- ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure
- ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes