Compliance & Risks

A New Era of Product Cybersecurity: 2026 Global Updates and Compliance Strategies

Author:

Giselle Chia, Regulatory Compliance Analyst
Compliance & Risks

16th April, 2026

Further regulatory developments may have occurred after publication. To keep up-to-date with the latest compliance news, sign up to our newsletter.

Table of Contents

A New Era of Product Cybersecurity: 2026 Global Updates and Compliance Strategies

Table of Contents

A New Era of Product Cybersecurity: 2026 Global Updates and Compliance Strategies

01. About The Author

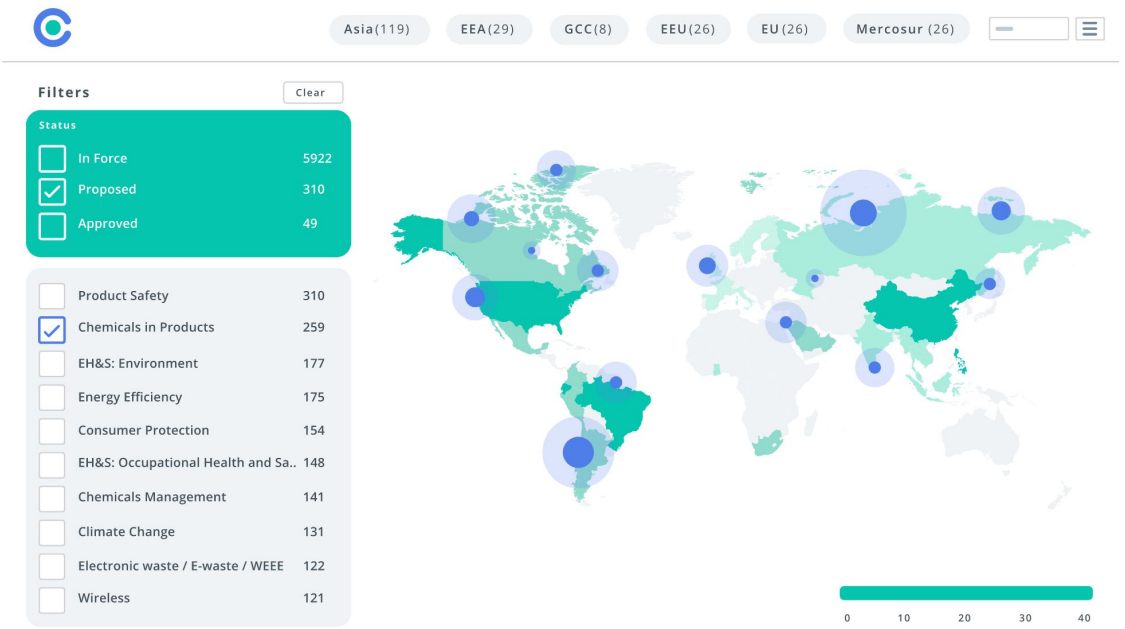
Giselle Chia
Regulatory Compliance Analyst, Compliance & Risks

Giselle is a Regulatory Compliance Analyst at Compliance & Risks. Since joining in 2023, she is responsible for monitoring the regulatory developments in Taiwan and ASEAN countries. She assists clients with their global compliance challenges with particular focus in the areas of Cybersecurity, Ecolabelling, Transport of Dangerous Goods and Construction Products.

Giselle holds a Honours Bachelor of Laws (LL.B.) and a Barrister-at-Law Degree from the Honorable Society of King's Inns, Ireland. She is a Mandarin native speaker who also speaks fluent English, Bahasa Malaysia/Indonesia and Cantonese.

02. Unlocking Market Access

At Compliance & Risks, we help you keep on top of global regulatory changes and their impact worldwide. We have the right technology, regulatory content and expertise to help you unlock market access, protect revenue and elevate the role of compliance.



Our solution includes:

- **C2P:** The most advanced product compliance and ESG compliance software on the market, helping you streamline your compliance process and unlock market access around the world.
- **Regulatory Content:** We provide the broadest and most comprehensive product compliance regulatory content on the market, monitoring 195+ countries, 20 industry sectors, 45 topics and 100,000+ regulatory sources.
- **Ask our Experts:** Direct access to our team of experts for support

Additionally, we offer:

- ✓ **Market Access Services:** Our Market Access team helps you understand your product compliance obligations by transforming regulations into actionable knowledge with tailored advice for you and your business.

Why choose C2P?

- ✓ **Stay ahead** of regulatory changes with the world's most comprehensive regulatory database
- ✓ **Avoid delays** with alerts of changes to regulations & requirements in real time
- ✓ **Improve efficiency with powerful collaboration and workflow tools** to keep compliance evidence up-to-date & live linked back to Regulations, Standards & Requirements

Contact us to speak to one of our team today to learn how you can simplify your regulatory compliance process.

For more information, please visit http://www.complianceandrisks.com

03. Introduction

This whitepaper examines the evolving regulatory landscape of product cybersecurity across the globe.

The primary focus of this policy area is the security of products with network connectivity, commonly defined as hardware, software, their components, and integral solutions that can connect to a network like the Internet or other devices for data communication and exchange. The entry into force of the UK's ***Product Security and Telecommunications Infrastructure Act 2022*** and its associated regulations, ***Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023***, on 29 April 2024 represents a decisive shift toward mandatory resilience in the face of escalating global cyber risks. Meanwhile, the global landscape is becoming increasingly intricate as different regions introduce diverse yet often overlapping security requirements.

This analysis will delve into key pieces of mandatory legislation that have been proposed, enacted, and taken effect over the past two years. Additionally, the whitepaper will explore voluntary schemes that promote cybersecurity labelling and certification as a means to enhance product security. This is your essential guide to product cybersecurity developments across key jurisdictions, including the EU, US, Australia, Japan, China, Taiwan, and Indonesia between 2024 and 2026.

*Note: This whitepaper is an update to the existing whitepaper, **A New Era of Product Cybersecurity: Navigating Regulatory Developments in 2024-2025**, published in May 2025.*

04. Key Product Cybersecurity Legislations

4.1. Australia

Cyber Security Act 2024

Australia's **Cyber Security Act 2024** represents a significant legislative step in enhancing the nation's cybersecurity framework. Enacted as a part of a broader Cyber Security Legislative Package, this Act introduces several critical measures aimed at bolstering protections for businesses, individuals and critical infrastructure against the rising tide of cyber threats. Among others, Part 2 of the Act confers power on the Minister of Home Affairs to prescribe rules to establish mandatory security standards for products that can directly or indirectly connect to the internet or a network ('relevant connectable products') that will be acquired in Australia.

Accordingly, manufacturers and suppliers of products subject to a security standard have a number of obligations:

- Manufacturers are obliged to manufacture the products in compliance with the security standard, and comply with any other requirements as set out in the security standard. They are also responsible for preparing, providingand retaining a statement of compliance for the supply of products.
- Suppliers must supply the products with a statement of compliance.

In cases of reasonably suspected non-compliance with the obligations, the Act stipulates a range of enforcement notices that may be served upon a manufacturer or supplier, these include compliance notice, stop notice, and recall notice. Remarkably, failure to comply with a recall notice may result in the public notification by the Minister.

Cyber Security (Security Standards for Smart Devices) Rules 2025

Swiftly following the enactment of the **Cyber Security Act 2024**, the Australian Minister for Home Affairs adopted the **Cyber Security (Security Standards for Smart Devices) Rules 2025**. The rules establish security standards for consumer grade products that are intended to be used, or are of a kind likely to be used for personal, domestic or household use or consumption,

,

such as smart TVs, smart watches, home assistants, baby monitors, and consumer energy resources. Crucially, desktop computers, laptops, tablet computers, smartphones, therapeutic goods, road vehicles and road vehicle components are explicitly excluded from the scope of application.

The standards closely adheres to UK's **Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023**, enacted under the **Product Safety and Telecommunications Act 2022**. Premised on the first 3 principles of **ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements),** the standards outline detailed requirements in relation to:

- Password: Passwords must be unique per product or defined by the user.
- Publication for reporting security issues: Manufacturers must publish information on how security issues are to be reported.
- Defined support period publication and security updates: Manufacturers and suppliers must publish information about the defined support period in which security updates will be provided.

The rules also prescribe the requirements for statement of compliance, setting out the information that shall be included. A statement of compliance shall be retained for at least 5 years under these standards.

2026 Updates

UK Compliance vs. Australian Compliance

Following the end of the 12-month grace period, the rules officially came into full force on 4 March 2026. In practice, businesses are always asking this same high-stake question: Does compliance with the UK regulations automatically mean that my product complies with the Australian rules?

The Australian regulations are closely aligned with the UK regulations. If your product already complies with the UK regulations, this will provide a strong foundation for meeting the Australian requirements.

However, Australia's framework has its own documentation requirements and enforcement mechanisms, meaning that manufacturers will still need to undergo an Australia-specific compliance and administrative process. In the FAQs Collection for the Australian rules, the Australian Ministry of Home Affairs has explicitly confirmed that the UK statement of compliance is acceptable for the Australian market, provided that the document is updated to satisfy all requirements of the Australian Act and Section 9 of the rules. Therefore, businesses must ensure that they understand any specific differences.

4.2. European Union

Cyber Resilience Act 2024

Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act) is a groundbreaking piece of legislation designed to bolster the cybersecurity of digital products placed on the EU market. The primary goal of the CRA is to ensure that digital products are secure by design and throughout their lifecycle. Think of it this way: from smartwatches and baby monitors to routers and software applications, an increasing number of products in our lives have digital components, making them potential entry points for cyber threats. The CRA steps in to address the currently fragmented and often inadequate cybersecurity measures in these products, thereby protecting consumers and businesses from growing cyber threats.

Broad Scope of Application: The CRA has a broad scope, covering virtually all products with digital elements (tangible or intangible) whose intended purpose or foreseeable use includes a direct or indirect connection to another device or network. This includes:

- Hardware (e.g. IoT/smart/connected devices, computers, laptops, smartphones, routers, industrial control systems etc.).
- Software (e.g. operating systems, applications, firmware etc.).
- Remote data processing solutions of an in-scope product, the absence of which would prevent the product from performing one of its functions (i.e. integral to the product's core functionality).
- Components, hardware or software, intended for integration into an in-scope product.

Exclusions: The CRA does not apply to the following products:

- Products covered by other EU regulations (medical devices, in vitro diagnostic medical devices, motor vehicles, civil aviation equipment, motor vehicles, marine equipment).
- Spare parts to replace identical components.
- Products developed or modified exclusively for national security or defence purposes.
- Products specifically designed to process classified information.

Manufacturer Obligations: The CRA shifts the responsibility towards manufacturers to ensure their products are secure by default. In essence, manufacturers must prioritize security from the design and development phase and maintain it throughout the product's entire lifecycle. They are required to:

- Design and develop products with essential cybersecurity requirements by default and by design.
- Implement procedures to address vulnerabilities and provide security updates for a defined support period.
- Design and develop products with processes in place to handle vulnerabilities discovered after the product is placed on the market.
- Provide instructions and information necessary for the secure use of the product.

- Report actively exploited vulnerabilities and incidents without undue delay to the relevant authorities (national CSIRTs and the EU Agency for Cybersecurity - ENISA).

- Conduct conformity assessments before placing products on the market and draw up technical documentation.
    -
- Affix the CE marking to products demonstrating conformity.

- Cooperate with competent authorities regarding any non-compliance.

Obligations of Importers and Distributors: The CRA also outlines detailed responsibilities of importers and distributors. Essentially, both importers and distributors act as gatekeepers, ensuring that only compliant products reach the EU market. Their main responsibility is to verify the manufacturer's compliance and to raise concerns if they identify any issues.

Important and Critical Products: Under the CRA, "important" and "critical" products are considered to pose a higher cybersecurity risk and thus subject to more stringent conformity assessment procedures. The key determining factor depends heavily on the core functionality of the product, namely the fundamental features and capabilities that fulfil the primary purpose for which the product has been made available, and without which the product would not be able to meet its intended use. The “important product” category covers products with direct implications for the security of another product, network or service, or products that carry a significant risk of adverse effects in terms of their intensity and ability to disrupt, control or cause damage to a large number of other products or to the health, security or safety of their users through direct manipulation. The “critical product” category covers products with highly specialized security-focused digital elements as a core function rather than just having security features. The European Commission is currently finalizing the technical description of the product categories, with its draft regulation released in March 2025. Through *Implementing Regulation (EU) 2025/2392* of December 2025, the European Commission finalises the technical description of the categories of important and critical products.

CRA's Implementation Timeline:

- 10 December 2024: The CRA entered into force.

- 11 June 2026: Obligations for Member States to appoint and notify of conformity assessment bodies will apply.

- 11 September 2026: Obligations for manufacturers to report actively exploited vulnerabilities and incidents will apply.

- 11 December 2027: 3-year transitional period ends. The main obligations of the CRA will fully apply. Products placed on the market after this date must comply with the CRA requirements.

2026 Updates

Commission Issued FAQs and Draft Guidance

The CRA establishes a precedent as the world's first comprehensive horizontal cybersecurity framework for digital products. It sparks significant questions regarding its practical implementation across the EU and the rest of the world, as it does not just impact EU businesses, but businesses worldwide that place such products on the EU market.

The CRA establishes a precedent as the world's first comprehensive horizontal cybersecurity framework for digital products. It sparks significant questions regarding its practical implementation across the EU and the rest of the world, as it does not just impact EU businesses, but businesses worldwide that place such products on the EU market.

More than a year after its adoption, the European Commission finally published the FAQs Collection for the CRA in December 2025. Subsequently in March 2026, the long-awaited Draft Guidance was released for public consultation. These two documents address the common practical implementation concerns, providing the much needed clarity for manufacturers and other stakeholders about their obligations under the new legislation..

Here are some of the most important questions answered regarding the actual application of the CRA:

Q: If I sell a hardware product but the essential control app is downloaded separately from an app store, is the app part of the hardware product?
A: Yes. If the software is necessary for the product to perform its intended functions, they together constitute a single "product with digital elements", even if the software is obtained through a separate channel like an app store or a download link after the hardware has been placed on the market.
Q: Do I need to completely redesign products already placed on the market before the CRA entered into application?
A: Not necessarily. Manufacturers must carry out a cybersecurity risk assessment to determine if the existing product meets the essential requirements. If the assessment shows the product already incorporates effective security measures for its intended use, the manufacturer can rely on those existing measures to demonstrate compliance with the CRA. However, the manufacturer must still fulfill all other obligations, such as drawing up an EU declaration of conformity, affixing the CE marking, and following vulnerability handling processes before placing new units of that legacy design on the market after the CRA applies.
Q: How do I determine the length of the support period for my product?
A: This period is determined based on the reasonably foreseeable lifetime of the product. The CRA generally mandates a support period of at least five years for all products, but this is a minimum safeguard, not a default. A support period shorter than five years is permitted if the product's expected use time is actually shorter than five years. Vice versa, if a product is expected to remain in use for ten years, the manufacturer should align the support period with that duration.

Non-EU Nations Mirroring CRA

The CRA's influence is already sparking the "Brussels Effect", where non-EU nations adopt similar frameworks to avoid market fragmentation. **Switzerland** is positioning itself at the forefront of international regulatory alignment by actively pursuing the mirroring of the CRA.

Currently, the Swiss **Telecommunications Installations Implementing Ordinance (OOIT)** regulates the cybersecurity requirements for connected radio equipment in alignment with the RED Delegated Act. The absence of such requirements for digital products on the horizon has been frequently raised in the Swiss Parliament. In August 2025, the Swiss Federal Council tasked the Federal Department of Defence, Civil Protection and Sport (DDPS) with drafting a bill regarding the Cyber Resilience of Digital Products to be submitted for consultation by autumn 2026. This new legislation will establish cybersecurity requirements for the development and commercialisation of products with digital components (including software and hardware), set out market surveillance rules, and lay the groundwork for prohibiting the import and sale of insecure devices. It will take into consideration the international context, especially the EU CRA, to minimise conflicting requirements and the administrative burden on businesses.

Vulnerability and Incident Reporting Kicks Off in September 2026: Where, When, and How?

Where: ENISA's new Single Reporting Platform (SRP) is to be used for the reporting of actively exploited vulnerabilities and severe incidents affecting the security of products with digital elements operating within the EU market.

When: The SRP will be operational from 11 September 2026, coinciding with the date when the mandatory reporting obligations for manufacturers officially enter into application. Manufacturers must follow a three-stage reporting timeline:

- Early warning: within 24 hours of becoming aware of the vulnerability or incident;
- Notification: within 72 hours of becoming aware, providing general information and an initial assessment;
- Final report: for vulnerability, within 14 days after taking a corrective measure; for incident, within 1 month from the notification.

How: Manufacturers submit notifications electronically through the SRP, which automatically routes them to the designated CSIRT coordinator (based on the manufacturer's main establishment) and ENISA simultaneously. The CSIRT then disseminates the information without delay to other relevant CSIRTs in Member States where the product is available, and to market surveillance authorities as needed.

Incoming Harmonised Standards for Products with Digital Elements in Support of the Cyber Resilience Act

In February 2025, the European Commission made a request (Standardisation Request M/606) to the CEN, CENELEC, and ETSI to develop new harmonised standards for products with digital elements to facilitate the implementation of the CRA. The standardisation request includes the development of 41 standards: 15 horizontal standards applicable to all products within the CRA's scope and 26 vertical standards specific to certain product categories (Important Class I, Important Class II, and Critical Class). These standards will translate the broad essential cybersecurity requirements of the CRA into detailed technical specifications. This will give manufacturers concrete guidance on how to design, develop, and produce secure products.

While subject to change, current information suggests that the first sets of standards are expected to be finalised in the lead-up to the CRA's full application date of 11 December 2027. The exact publication dates for all these standards in the OJEU remain unavailable, but the European Commission has set the following adoption deadlines for the ESOs:

- Horizontal standards: 30 August 2026 and 30 October 2027
- Vertical standards: 30 October 2026

2026 Updates

CRA Standardisation Progress

In April 2025, the three ESOs officially accepted the standardisation request. At CEN and CENELEC, several working groups have been established to lead on the development of horizontal standards: CEN-CLC/JTC 13 WG 9 and WG 6, CEN/TC 224 WG 17, CLC/TC 65X WG 3, and CLC/TC 47X. A new dedicated group, ETSI EUSR, has also been established within the ETSI TC CYBER to work on the delivery of vertical standards.

Horizontal Standards:

CEN-CLC/JTC 13 WG 9 is developing the new **EN 40000** series which is applicable to all categories of products with digital elements. Serving as the cornerstone of the CRA, the series is structured into four primary parts, each addressing a specific pillar of the essential requirements:

- prEN 40000-1-1 **Cybersecurity requirements for products with digital elements - Vocabulary**
  Specifies the terms and definitions commonly used in the series.

- prEN 40000-1-2 **Cybersecurity requirements for products with digital elements - Part 1-2: Principles for cyber resilience**
  Specifies general cybersecurity principles and risk management activities, covering every stage of the product lifecycle.

- prEN 40000-1-3 **Cybersecurity requirements for products with digital elements Part 1-3: Vulnerability Handling**
  Provides specifications applicable to vulnerability handling processes to be put in place by manufacturers.

- prEN 40000-1-4 **Cybersecurity requirements for products with digital elements Part 1-4: Generic Security Requirements**
  Provides generic technical cybersecurity requirements for products with digital elements.

As of April 2026, **prEN 40000-1-1 (Vocabulary), prEN 40000-1-2 (Cyber Resilience Principles),** and **prEN 40000-1-3 (Vulnerability Handling)** have undergone public enquiry and are currently under approval. The drafts are available at the German Institute for Standardization (DIN, the Secretariat of CEN/CLC/JTC 13)'s website, DIN Media:

- DIN EN 40000-1-1:2026-03 - Draft
- DIN EN 40000-1-2:2026-03 - Draft
- DIN EN 40000-1-3:2026-02 - Draft

prEN40000-1-4 (Generic Security Requirements) is still under drafting. Importantly, it is named as the central standard of the horizontal EN 40000 series. It is structured along the 13 essential requirements (Annex I, Part I, Article 2(a) through (m)) of the CRA, establishing a coherent library of security controls, their objectives, and corresponding assessment criteria. It builds upon the EN 18031 series originally developed to address the Radio Equipment Directive's essential cybersecurity requirements, augmented with additional security controls to cover the scope of CRA. Earlier in March 2026, CEN and CENELEC co-hosted an online deep dive session covering the current state of prEN 40000-1-4. Event details, presentation and recording can be accessed here: CRA Standards Unlocked: Deep Dive Session Security Controls - Generic security requirements.

Vertical Standards:

As of April 2026, the ETSI EUSR are finalising the **EN 304 6XX** series. The drafts are publicly and freely available on the ETSI Open Area for public consultation. The series covers 18 product categories:

- EN 304 617 Browsers
- EN 304 618 Password managers
- EN 304 619 Software that searches for, removes, or quarantines malicious software (Antivirus)
- EN 304 620 Virtual Private Networks (VPNs)
- EN 304 621 Network Management Systems (NMS)
- EN 304 622 Security Information and Event Management (SIEM) systems
- EN 304 623 Boot managers

- EN 304 624 Public Key Infrastructure (PKI) and digital certificate issuance software
- EN 304 625 Physical and virtual network interfaces
- EN 304 626 Operating Systems (OS)
- EN 304 627 Routers, modems intended for the connection to the internet, and switches
- EN 304 631 Smart home general purpose virtual assistants
- EN 304 632 Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems
- EN 304 633 Internet connected toys
- EN 304 634 Personal wearable products
- EN 304 635 Hypervisors and container runtime systems
- EN 304 636 Firewalls, intrusion detection and/or prevention systems
- EN 304 642 Network functions of telecommunications systems

Resources:

The STAN4CRA Projects, comprising STAN4CR and STAN4CR2, are European initiatives funded by the European Innovation Council and SMEs Executive Agency (EISMEA) and EFTA. The stan4cra.eu website updates information on the CRA standardisation activities. Manufacturers are encouraged to utilise the resource to track new developments and stay updated. Additionally, the cyberstand.eu platform has been established to help European stakeholders engage in the standardisation progress.

EN 18031 Series on Cybersecurity Requirements for Internet Connected Radio Equipment under the Radio Equipment Directive

EN 18031 is a series of harmonised standards developed by the CEN and CENELEC to address the essential cybersecurity requirements for certain categories of radio equipment which were introduced by Articles 3(3)(d), (e) and (f) of **Directive 2014/53/EU (Radio Equipment Directive)** and further elaborated by **Delegated Regulation (EU) 2022/30 (RED Delegated Regulation on Cybersecurity)**. The long-awaited series was adopted by the ESOs in August 2024, and officially published in the OJEU through **Commission Implementing Decision (EU) 2025/138** in January 2025.

The series consists of three standards:

- **EN 18031-1:2024** Common security requirements for radio equipment - Part 1: internet connected radio equipment
- **EN 18031-2:2024** Common security requirements for radio equipment - Part 2: radio equipment processing data, namely internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment
- **EN 18031-3: 2024** Common security requirements for radio equipment - Part 3: internet connected radio equipment processing virtual money or monetary value

Delegated Regulation (EU) 2022/30) became fully applicable from 1 August 2025. Compliance with these standards, within the stated restrictions, confers a presumption of conformity with the essential requirements established by the RED and the Delegated Regulation.

2026 Updates

Repeal of Delegated Regulation (EU) 2022/30 (RED Delegated Regulation on Cybersecurity)

On 16 February 2026, the European Commission published the final version of the *Delegated Regulation repealing Delegated Regulation (EU) 2022/30* (publication in the OJEU will follow shortly). The primary objective of the repeal is to avoid regulatory overlap with the CRA's

essential requirements that fully cover the cybersecurity elements previously addressed under RED Articles 3(3)(d), (e), and (f), and create a clear path for regulatory transition to the CRA framework. The repeal will take effect on 11 December 2027, coinciding with the full applicability of the CRA.

From 1 August 2025 until 10 December 2027, in-scope radio equipment placed on the EU market must still comply with the RED requirements. From 11 December 2027 onwards, all products with digital elements, including radio equipment, must comply with the CRA requirements.

The Commission has also indicated that references to RED cybersecurity standards, namely the EN 18031 standards, will be removed from the OJEU. The implication is that the standards will no longer have legal standing for presumption of conformity with the RED. However, the work invested in achieving EN 18031 compliance remains valuable; it is a crucial stepping stone for CRA readiness, because the forthcoming EN 40000 standards for CRA compliance will incorporate the existing EN 18031 standards.

.

CE Marked Radio Equipment on the UK Market

The requirements for radio equipment differ between Northern Ireland (NI) and Great Britain (GB), primarily due to the Windsor Framework and the interaction between EU regulations and the UK's domestic security regime. See UK's Statutory Guidance for Regulation (EU) 2022/30.

NI Market: From 1 August 2025, the NI market is governed by Regulation (EU) 2022/30. Radio equipment that is supplied in NI must meet additional cybersecurity, privacy, and fraud protection requirements. They are generally excepted from the UK's PSTI regime. These rules are applied to facilitate NI's unique position with access to both the UK internal market (unfettered access).

GB Market: For CE marked radio equipment placed on the GB market from 1 August 2025, manufacturers must navigate a "deemed compliance" model combined with domestic security laws. EU-compliant CE marked radio equipment is deemed to meet the essential requirements of the UK Radio Equipment Regulations 2017. Unlike in NI, radio equipment in GB must also meet the UK's PSTI security requirements, regardless of its CE status. Manufacturers supplying the GB market must provide a specific Statement of Compliance regarding these PSTI requirements.

4.3. Indonesia

Draft Law on Cyber Resilience and Security (RUU KKS)

Discussions on the need for cybersecurity legislation in Indonesia have been ongoing for some time. In 2019, the Indonesian House of Representatives (DPR) officially introduced the Draft Law on Cyber Security and Resilience (RUU KKS) for the first time. However, progress on its development and ratification remained minimal. In November-December 2024, efforts to include RUU KKS as a priority in the 2025 National Legislation Program (Prolegnas) received significant support from the legislative body. As a result, the Indonesian Government is currently finalising the draft, with its latest version issued in February 2025.

RUU KKS aims to establish a comprehensive legal framework for cybersecurity and resilience in ndonesia by addressing various aspects that include the governance of products with digital elements (PDED). Having strong resemblance to the EU's CRA, PDED is defined in the same way as the "Product with Digital Elements" under the EU legislation. It refers to a software or hardware product and its remote data processing solutions, including software and hardware components being put on the market separately. PDED is classified into three risk levels - standard, medium and high.

Assessment and Certification of PDED:

- Standard PDED does not require certification or assessment by the National Cyber Agency. However, they must conduct self-assessment before being marketed and/or used.
- Medium-risk and high-risk PDED are subject to mandatory third-party assessment by the National Cyber Agency before being marketed and/or used. They would be assessed against security standards and obtain a certificate upon successful assessment. Further provisions regarding PDED, assessment guidelines and security standards will be determined by the National Cyber Agency through regulations.

Obligations of PDED Manufacturers: The manufacturers of PDED have a number of obligations in ensuring the security of their products. For instance, they must:

- Identify and document the strengths, vulnerabilities, and components contained in the product, and compile a list of software used;
- Address and remediate vulnerabilities, including providing security updates;
- Conduct regular security testing and evaluation of the PDED;
- When updates become available, disclose information about vulnerabilities that have been addressed;
- Implement a coordinated vulnerability disclosure policy;
- Provide a secure mechanism for distributing security updates for PDED in a timely manner;
- Notify users about security update tools and the necessary actions to be taken;
- Ensure that their products continuously meet the PDED requirements set by the Government through further regulation.

PDED, AI and Data Protection: Artificial Intelligence developed, implemented, and/or produced by PDED manufacturers must comply with AI Ethics Principles, and must be reported to the National Cyber Agency. More specifically, the AI Ethics Principles that must be taken into consideration are:

- Inclusivity;
- Humanity;
- Security;
- Accessibility;
- Transparency;
- Credibility and accountability;
- Personal data protection;
- Sustainable development and Environment; and
- Intellectual property protection.

Enforcement Status: Upon adoption, the Cyber Security and Resilience Law is scheduled to enter into force on the day of its enactment. All implementation regulations of this law will be stipulated within 2 years from its effective date.

Key Insights:

The explicit resemblance of the RUU KKS's definition of PDED to the CRA's "Products with Digital Elements" and emphasis on product life security are a significant advantage for manufacturers already compliant with or preparing for the CRA. However, divergences will exist. The risk levels (standard, medium, and high) and the specific assessment and certification processes dictated by the Indonesian National Cyber Agency will likely have their own nuances and requirements.

The explicit inclusion of AI Ethics Principles is a notable and potentially leading aspect of the Indonesian legislation. Demonstrating adherence to these AI Ethics Principles could become a competitive advantage for manufacturers in the Indonesian market.

In conclusion, the Indonesian RUU KKS presents both familiar concepts and new specific requirements for manufacturers of products with digital elements. Looking ahead, although not a direct substitute, existing compliance efforts for the CRA will provide a significant head start in understanding the underlying principles and establishing necessary processes.

4.4. China

Proposed Mandatory National Standard on the Basic Requirements and Test Methods for Consumer Internet of Things Product Security

In March 2025, China proposed a mandatory national standard (GB) to establish the basic requirements for the security of consumer grade IoT products and corresponding test methods. The standard is currently subject to the preliminary drafting process, and China's Ministry of Industry and Information Technology (MIIT) is working towards releasing the draft for public consultation. According to the deliberation plan, the standard will apply to the research and development, design and production of the products, as well as the analysis, testing and evaluation of product safety functions. In relation to technical contents, it will describe the basic requirements and test methods for the following aspects:

- Vulnerability Report Management
- Software update and maintenance
- Minimization of attack surface
- System fault resistance
- Personal data deletion
- Device installation and maintenance
- Data protection

This standard aims to align China's practices with international best practices such as *ISO/IEC 27402NIST IR 8425:2023 (Cybersecurity - IoT security and privacy - Device baseline requirements), the US' NIST IR 8425 (Profile of the IoT Core Baseline for Consumer IoT Products), the EU's ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements) and ETSI TS 103 701 (Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements)*. It will also take into account the IoT security labels implemented by other countries including the US, Finland, Germany, and Singapore.

4.5. Taiwan

Proposed Cybersecurity Testing Requirements for Network Products and Audiovisual Products with Network Connectivity

In October 2025, the Taiwanese Bureau of Standards, Metrology and Inspection (BSMI) proposed to introduce cybersecurity testing requirements for network products, as well as IT and audiovisual products with network connectivity. From **1 January 2028**, both domestically produced and imported products must be inspected against the applicable cybersecurity standards.

Product Types	Inspection Standards for Cybersecurity
Network Products: • routers • bridges • switches • network hubs • gateways (including smart speakers and smart home assistants)	Wireless connectivity or both wireless and wired connectivity - (1) or (2) Wired connectivity only - (1) (1) CNS 16190 (2023) (2) CNS 18031-1 (2025), CNS 18031-2 (2025)
Network-Connected Digital Cameras	Wireless connectivity or both wireless and wired connectivity - (1), (2) or (3) Wired connectivity only - (1) or (2) (1) CNS 16120-1 (2022), CNS 16120-2 (2019), CNS 16132-1 (2022), CNS 16132-2 (2023) (2) CNS 16190 (2023) (3) CNS 18031-1(2025), CNS 18031-2 (2025)
Network-Connected Video Recorders	Wireless connectivity or both wireless and wired connectivity - (1), (2) or (3) Wired connectivity only - (1) or (2) (1) CNS 16120-1 (2022), CNS 16120-3 (2021), CNS 16132-1 (2022), CNS 16132-3 (2023) (2) CNS 16190 (2023) (3) CNS 18031-1 (2025), CNS 18031-2 (2025)

Product Types	Inspection Standards for Cybersecurity
Network-Connected Monitors	Wireless connectivity or both wireless and wired connectivity - (1) or (2) shall Wired connectivity only - (1) (1) CNS 16190 (2023) (2) CNS 18031-1 (2025), CNS 18031-2 (2025)
Network-Connected Televisions	Wireless connectivity or both wireless and wired connectivity - (1) or (2) Wired connectivity only - (1) (1) CNS 16190 (2023) (2) CNS 18031-1 (2025), CNS 18031-2 (2025)

05. Voluntary Labelling and Certification Schemes

5.1. EU: European Common Criteria-based Cybersecurity Certification Scheme (EUCC)

Entered into force on 27 February 2024, Regulation (EU) 2024/482 establishes the EU's cybersecurity certification scheme on Common Criteria (EUCC). Voluntary-based, the new scheme is mandated by the EU's cybersecurity certification cornerstone, Regulation (EU) 2019/881 (Cybersecurity Act). In order to harmonise cybersecurity certification within the EU, it is built upon the SOG-IS time-proven and internationally recognised 'Common Criteria' and 'Common Evaluation Methodology' already used across 17 Member States, namely ISO/IEC 15408 (Information security, cybersecurity and privacy protection — Evaluation criteria for IT security) and ISO/IEC 18045 (Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation).

The scheme applies to all Information and Communication Technology (ICT) products, including their protection profiles as part of the ICT process. Based on third party evaluation, it evaluates the inherent security capabilities and assurance levels ('substantial' and 'high') of these products. One year after its publication, the EUCC entered into application on 27 February 2025.

Possibility of Implementing Cyber Resilience Act through EUCC:

The European Union Agency for Cybersecurity (ENISA) is exploring the idea of leveraging the existing EUCC framework to demonstrate compliance with the CRA.

The CRA provides manufacturers with various options for demonstrating compliance with its essential requirements. These pathways include utilising European cybersecurity certification schemes like the EUCC, as well as adhering to harmonised standards and undergoing recognised conformity assessment procedures. Notably, the CRA grants a "presumption of conformity" to products certified under a recognised European scheme, such as the EUCC, if the certification meets at least a "substantial" assurance level, as outlined in Article 27. It is important to note, however, that EUCC certification is not a mandatory prerequisite for CRA compliance, even for products deemed important or critical. Instead, it serves as one of several available routes for manufacturers who wish to leverage the EUCC's structured conformity processes to meet the CRA's demands.

A study conducted by ENISA, with report finalised in January 2025, delves into the technical elements required to bridge the gap between EUCC and CRA, suggesting a practical and detailed approach to achieving this synergy. Still exploratory, ENISA is actively facilitating the EUCC/CRA alignment, and industry stakeholders are encouraged to participate in pilot implementations to evaluate its applicability and provide feedback.

5.2. US: Cybersecurity Labelling for Internet of Things Program (US Cyber Trust Mark)

In March 2024, the US Federal Communications Commission (FCC) established a framework for a voluntary cybersecurity labelling program for wireless consumer Internet of Things (IoT) products. Eligible products include internet-connected home security cameras, voice-activated shopping devices, smart appliances, fitness trackers, garage door openers, and baby monitors. The program does not apply to computers or smartphones.

The program will allow qualifying products that meet baseline cybersecurity criteria established by the National Institute of Standards and Technology (NIST) to display a FCC IoT Label that includes a new US government certification mark ("US Cyber Trust Mark") and an accompanying QR code linked to a dynamic, decentralised, publicly available registry of more detailed cybersecurity information. This easy-to-understand and quickly recognisable label will assist consumers assess a product's cybersecurity, identify trustworthy products and make informed purchasing decisions.

The program will rely on public-private collaboration, with the FCC providing oversight and approved third-party Cybersecurity Label Administrators (CLAs) managing activities such as evaluating product applications, authorizing use of the label, and supporting consumer education. Compliance testing will be handled by accredited laboratories, CyberLABs. As the FCC pushes ahead with the novel program, UL Solutions and 10 other entities were announced as CLAs in December 2024, with UL Solutions serving as the Lead Administrator (LA).

While the framework is in place, the program is not yet officially launched. To ensure an effective rollout, the FCC is currently working on specific implementation details and will further seek public input as it progresses. The FCC is also working with other federal agencies to achieve international recognition of the FCC IoT Label and mutual recognition of international labels. This new federal initiative can be expected to roll out this year, as a White House official affirmed in January 2025 that "there will be labelled products on the shelves in 2025."

5.3. Japan: Labelling Scheme based on Japan Cyber-Security Technical Assessment Requirements (Japan Cyber STAR / JC-STAR)

JC-STAR is a Japanese labelling scheme operated by the Information-Technology Promotion Agency (IPA) that confirms the conformance of IoT products to security technical requirements based on its own standards, while also harmonising with domestic and international standards such as ETSI EN 303 645 and NISTIR 8425. The scheme covers a wide range of IoT products with the ability to send and receive data over the Internet using Internet Protocol (IP), including products that are indirectly connected to the Internet. General-purpose IoT products, such as PCs, smartphones, tablets, etc. that can have security features added after purchase are not covered by the scheme.

The scheme is a voluntary multi-level scheme:

- STAR-1 is a unified baseline that establishes security requirements that address minimum threats common to all IoT products.
- STAR-2, STAR-3 and STAR-4 establish security requirements per product category to address characteristics of each product category.

For STAR-1 and STAR-2, conformance labels will be granted by the IPA based on self-declarations of conformity. For STAR-3 and STAR-4, labels will be granted based on third-party evaluations by independent test laboratories, as the products are intended for use in procurement by government agencies and critical infrastructure providers, and therefore require high reliability. Administrator (LA).

A label remains valid for 2 years, and IoT products that obtain the label can affix it on the product itself, its packaging, etc. The label contains a QR code with embedded URL that links to the website managed by the IPA, listing labelled products under its management and providing up-to-date information relating to the vendor, product and label, as well as product security information (updates, vulnerability, etc.) and relevant contact details.

On 25 March 2025, the IPA officially launched the scheme and started accepting applications for STAR-1. Conformance criteria for STAR-2 and above is being developed with a focus on two priority product categories: network cameras and network devices. The IPA plans to begin accepting applications for STAR-2 and above of these two product categories after January 2026. In the meantime, the Japanese Ministry of Economy, Trade and Industry (METI) will continue to pursue interoperability and mutual recognition with schemes of other countries to reduce the cost burden of vendors when exporting IoT products. Specifically, METI will continue negotiations with foreign authorities for mutual recognition with Singapore (Cybersecurity Labelling Scheme), the UK (PSTI Act), the US (Cyber Trust Mark), and the EU (Cyber Resilience Act).

2026 Updates

In March 2026, a Memorandum of Cooperation (MoC) on the mutual recognition of IoT cybersecurity schemes was signed between Japan and Singapore. Effective 1 June 2026, smart devices (smart home assistants, home automation and alarm systems, IoT gateways and hubs that connect multiple devices) that have obtained cybersecurity labels under Japan's JC-STAR scheme and Singapore's Cybersecurity Labelling Scheme (CLS) will be mutually recognised, allowing manufacturers to apply for the other country's labelling scheme through a streamlined process.

5.4. China: Proposed Cybersecurity Labelling Scheme (China Cybersecurity Label)

In November 2025, the Cyberspace Administration of China (CAC) proposed the *Administrative Measures for Cybersecurity Labelling* targeting all products with internet connectivity functions. Participation is voluntary, where manufacturers are encouraged to label their products and consumers are encouraged to prioritise products that carry the label.

The **China Cybersurity Label** classifies capabilities into three levels indicated by stars: basic (one star), enhanced (two stars), and leading (three stars).

- The basic level requires meeting fundamental national standards like avoiding weak passwords, establishing a vulnerability management mechanism, and maintaining software updates.
- The enhanced level requires that a product's cybersecurity capabilities reach an advanced domestic level.
- The leading level requires meeting advanced international level while also passing penetration testing to demonstrate the ability to withstand high-level cyberattacks.
- For the first batch, the measures specifically apply to consumer networked cameras intended for individual and home use.

Deemed Compliance with the UK PSTI Security Requirements

In December 2025, the UK Department for Science, Innovation and Technology issued the ***Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) (Amendment) (No.2) Regulations 2025*** *(Statutory Instrument No. 1267 of 2025)*.

The regulations officially recognises two international cybersecurity standards from Japan and Singapore as meeting UK security requirements for connectable products. A manufacturer is now treated as having complied with UK security requirements and the mandate for a statement of compliance if their product:

- *holds a current, non-expired conformance label under **Japan JC-STAR STAR-1;** or*
- *holds a current, non-expired label under any level of the Singapore **Cybersecurity Labelling Scheme**.*

06. Conclusion

The year 2026 marks a decisive operational phase in the evolution of product cybersecurity, solidifying the global shift from voluntary guidelines to mandatory, lifecycle-based security frameworks. While the foundational legislation like the EU's landmark CRA, the UK's PSTI regime, and Australia’s fully operational Cyber Security Act have been established, 2026 brings critical clarity and implementation deadlines.

The CRA is rapidly moving into practice, driven by the European Commission's release of FAQs (December 2025) and Draft Guidance (March 2026) to clarify practical obligations. A key milestone is the mandatory vulnerability and incident reporting, which commences on 11 September 2026, utilising ENISA’s new Single Reporting Platform (SRP). Simultaneously, the groundwork for harmonised standards is accelerating, with the horizontal EN 40000 series and the vertical EN 304 6XX series progressing toward finalisation to give manufacturers concrete technical guidance for compliance. This drive for coherence also involves regulatory clean-up, such as the repeal of the RED Delegated Regulation (EU) 2022/30 by December 2027 to eliminate overlapping requirements.

Globally, the interconnected nature of compliance is becoming more concrete. While Australia's rules are now fully in force (March 2026), manufacturers must be aware that UK compliance serves as a strong starting point but requires Australia-specific documentation and administrative processes. Conversely, the UK has explicitly paved a path for "deemed compliance" by recognising international schemes like Japan's JC-STAR STAR-1 and the Singapore Cybersecurity Labelling Scheme. This pragmatic recognition shows a global trend toward interoperability while regions like Switzerland mirror the CRA.

The focus for manufacturers has shifted from understanding the “what” to mastering the “how”. Compliance is now a continuous operational necessity, requiring the adoption of security-by-design principles, robust vulnerability handling procedures, and meticulous documentation. Leveraging voluntary schemes not only demonstrates commitment but can also expedite the mandatory conformity assessment process. Businesses that actively monitor legislative developments, participate in standardisation progress, and transform security from a reactive measure into a strategic product differentiator will secure both market access and customer trust in this new, fully regulated digital era.

Compliance & Risks

OUR NUMBERS

300+

CUSTOMERS WORLDWIDE

195

COUNTRIES COVERED

115,000+

REGULATIONS