Compliance & Risks

A New Era of Product Cybersecurity: Navigating Regulatory Developments in 2024-2025

Author:

Giselle Chia, Regulatory Compliance Analyst
Compliance & Risks

12th May, 2025

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

→ | complianceandrisks.com

Table of Contents

A New Era of Product Cybersecurity: Navigating Regulatory Developments in 2024-2025

01. About The Author

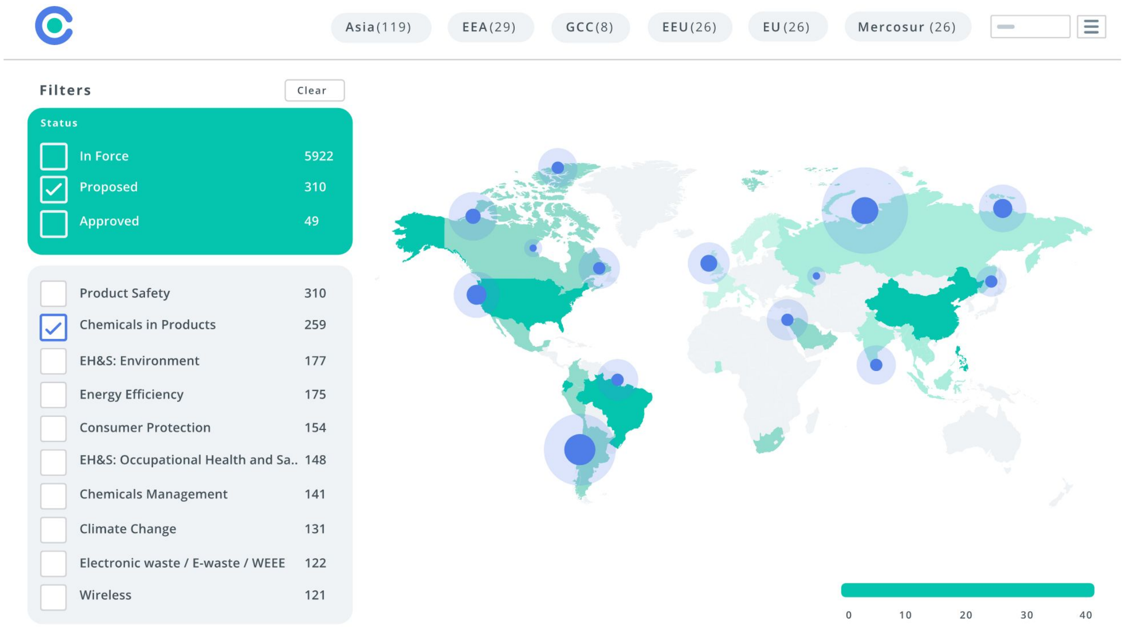
Giselle Chia
Regulatory Compliance Analyst,
Compliance & Risks

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.



Asia(119) | EEA(29) | GCC(8) | EEU(26) | EU(26) | Mercosur (26)

Filters — Clear

Status

□	In Force	5922
☑	Proposed	310
□	Approved	49

□	Product Safety	310
☑	Chemicals in Products	259
□	EH&S: Environment	177
□	Energy Efficiency	175
□	Consumer Protection	154
□	EH&S: Occupational Health and Sa..	148
□	Chemicals Management	141
□	Climate Change	131
□	Electronic waste / E-waste / WEEE	122
□	Wireless	121

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

Important Notice: All information provided by Compliance & Risks Limited and its contributing researchers in this report is provided for strategic and informational purposes only and should not be construed as company-specific legal compliance advice or counsel. Compliance & Risks Limited makes no representation whatsoever about the suitability of the information and services contained herein for resolving any question of law. Compliance & Risks Limited does not provide any legal services.

03. Introduction

This whitepaper examines the evolving regulatory landscape of product cybersecurity across several key jurisdictions: Australia, the EU, Indonesia, China, the US, and Japan.

The primary focus is on products with network connectivity - including hardware, software, their components, and integral solutions - that can connect to a network like the internet or other devices for data exchange. This analysis will delve into key mandatory legislations that have been proposed, enacted, and taken effect in 2024 and the first two quarters of 2025. Additionally, the whitepaper will explore voluntary schemes that promote cybersecurity labeling and certification as a means to enhance product security.

In reality, the terms used to describe these products, including "Internet of Things (IoT) devices", "smart devices" and "connected devices", are often broad and lack a unified definition among experts. While the EU has recently enacted the *Cyber Resilience Act* to govern the cybersecurity of "products with digital elements", the UK and Australia utilize the term "relevant connectable products" in their respective legislations. These terms, while similar, contribute to the complexity of the regulatory environment.

The entry into force of the UK's *Product Security and Telecommunications Infrastructure Act 2022 (PSTI)* and its associated regulations, *Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023*, on 29 April 2024 marks a significant step. Simultaneously, the global landscape is becoming increasingly intricate as different regions introduce diverse yet often overlapping security requirements. This necessitates a globally aware and potentially more harmonized approach to product compliance.

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, providing and 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 standards 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.

Implications of the Australian Regulations and Actionable Recommendations

The Australian regulations are closely aligned with the UK regulations. If your business already complies with the UK regulations, this will provide a strong foundation for meeting the Australian requirements. However, businesses must ensure that they understand any specific differences. The *Cyber Security (Security Standards for Smart Devices) Rules 2025* were registered on 4 March 2025, and the 12-month grace period ends on 4 March 2026. To meet the requirements within the limited timeframe, businesses need to proactively assess the specific nuances of the Australian rules and implement any necessary adjustments to their products and compliance processes without delay.

The fundamental shift from universal default passwords to unique passwords for consumer smart devices means that manufacturers need to:

- Implement secure password generation and management processes during manufacturing.
- Provide clear and user-friendly instructions on how to set strong and unique passwords.

In relation to mandatory vulnerability reporting mechanisms, businesses can:

- Set up a dedicated channel (e.g. a security contact email or a vulnerability reporting form on your website).
- Establish internal processes for triaging, assessing, and addressing reported vulnerabilities.

To comply with the enhanced transparency regarding security update period, it is crucial to:

- Define realistic and supportable security update periods for your products, considering their lifecycle and potential vulnerabilities.
- Clearly communicate this information on product packaging, websites, and during the point of sale.

As regards the statement of compliance:

- Develop a process for generating and managing these statements of compliance.
- This will likely require internal testing and verification against the standards.

Prioritizing compliance is essential, as non-compliance can trigger significant operational disruptions, costly penalties, and lasting reputational damage that erodes customer trust and market standing.

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.

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.

Implications of the CRA and Strategic Outlook:

The CRA represents a pivotal step in fortifying the EU's digital ecosystem. Complementing NIS2's focus on the cybersecurity of essential and important entities, the CRA targets the foundational security of the products underpinning their operations and the digital lives of all users. This shift from a largely voluntary to a mandatory product cybersecurity framework signals a significant paradigm change. Given the EU's market size and influence, the CRA's impact will undoubtedly resonate globally, compelling manufacturers worldwide to adhere to its requirements for EU market access.

The CRA's holistic approach, mandating security considerations throughout the entire product lifecycle - from initial design to end-of-life - necessitates a fundamental re-evaluation of product development processes. Robust due diligence across increasingly complex supply chains becomes paramount, as manufacturers bear responsibility for the security of integrated components. Moreover, the enhanced transparency regarding security features and vulnerabilities will empower consumers and businesses to make more informed purchasing decisions, fostering a more security-conscious marketplace.

Strategically, the CRA presents a significant opportunity for forward-thinking businesses. Rather than perceiving it as a mere compliance obligation, organizations should recognize its potential to cultivate substantial customer trust - a critical differentiator in today's digital landscape. Embracing the CRA can translate into a distinct competitive advantage, enabling businesses to market products with demonstrably robust security credentials, potentially attracting security-conscious customers and partners.

Potential Challenges for All Affected Parties:

Despite the phased implementation timeline intended to facilitate adaptation, the novelty of the CRA introduces uncertainties and ambiguities concerning its interpretation and practical application. The exceptionally broad definition of "products with digital elements" presents a considerable challenge for manufacturers in accurately determining the precise scope of products falling under the CRA's purview. Furthermore, the development of harmonized standards across this extensive scope is an evolving process, adding another layer of complexity. The European Commission's indication of a new assessment method for CRA's harmonized standards, distinct from the traditional HAS assessment, further contributes to this uncertainty and necessitates a learning curve for stakeholders.

In these initial stages of the CRA's implementation, the complete contours of the compliance framework remain unsettled. Clarity will likely emerge gradually as more harmonized standards are developed and adopted, national enforcement practices take shape, and a consistent interpretation of the legislation solidifies across the EU. Consequently, manufacturers face the ongoing challenge of staying informed about these evolving developments and proactively engaging with emerging guidance to ensure timely and accurate compliance.

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

In February 2025, the European Commission made a request to the CEN, Cenelec, and ETSI to develop new harmonized standards for products with digital elements to facilitate the implementation of the CRA. The standardization 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 finalized 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

Recommendations for Manufacturers:

1. Monitor Standardization Activities: Closely follow the progress of CEN, Cenelec, and ETSI, and engage with the organizations if necessary.

2. Early Adoption: Start aligning the product development process with the essential requirements of the CRA even before the harmonized standards are finalized. A proactive approach will make the transition smoother.

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

EN 18031 is a series of harmonized 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 *Regulation (EU) 2022/30*. 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.

When the application of *Regulation (EU) 2022/30* becomes mandatory 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, as further specified by *Regulation (EU) 2022/30*.

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 finalizing the draft, with its latest version issued in February 2025.

RUU KKS aims to establish a comprehensive legal framework for cybersecurity and resilience in Indonesia 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 27402:2023 (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.

05. Voluntary Labeling & 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 harmonize cybersecurity certification within the EU, it is built upon the SOG-IS time-proven and internationally recognized '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 utilizing European cybersecurity certification schemes like the EUCC, as well as adhering to harmonized standards and undergoing recognized conformity assessment procedures. Notably, the CRA grants a "presumption of conformity" to products certified under a recognized 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 finalized 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 Labeling 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 labeling 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, decentralized, publicly available registry of more detailed cybersecurity information. This easy-to-understand and quickly recognizable label will assist consumers to 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 labeled products on the shelves in 2025."

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

JC-STAR is a Japanese labeling 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 harmonizing 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. 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 labeled 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 Labeling Scheme), the UK (PSTI Act), the US (Cyber Trust Mark), and the EU (Cyber Resilience Act).

06. Conclusion

The product cybersecurity landscape is undergoing a rapid transformation, driven by evolving threats and increasingly stringent regulatory requirements across major global markets.

As evidenced by the recent legislative actions in Australia, the EU, and the proposed regulations in Indonesia and China, a clear trend towards mandatory security standards for connected devices is emerging. The UK's *Product Security and Telecommunications Infrastructure Act 2022*, Australia’s *Cyber Security Act 2024*, and the EU's groundbreaking *Cyber Resilience Act 2024* exemplify this shift, setting new benchmarks for manufacturers worldwide.

Manufacturers must now proactively integrate security by design principles into their product development lifecycles, address vulnerabilities promptly, and provide transparent security updates. The harmonization efforts, exemplified by the EU's pursuit of harmonized standards and the alignment of Australia’s regulations with the UK’s, suggest a potential pathway to greater global interoperability. However, regional nuances and specific local requirements, such as Indonesia’s focus on AI ethics and China’s proposed technical standards, will necessitate careful consideration.

Furthermore, voluntary labeling and certification schemes, like the EUCC, the US Cyber Trust Mark, and Japan’s JC-STAR, offer avenues for businesses to demonstrate their commitment to cybersecurity and gain a competitive edge. These schemes can also potentially ease the path to mandatory compliance.

In this complex and evolving environment, proactive engagement - staying informed, adapting quickly, and embracing a security-first approach - is no longer optional but essential for sustained market access and long-term prosperity. Businesses that prioritize security and transparency will not only mitigate risks but also cultivate deeper customer trust and unlock opportunities in an increasingly interconnected digital world. The coming years will demand continuous vigilance regarding legislative developments, active participation in standardization initiatives, and an unwavering commitment to robust security practices throughout the entire product lifecycle, transforming security from a cost center into a strategic differentiator.

Want to stay ahead of your cybersecurity compliance obligations? Start a Conversation now!

Compliance & Risks

OUR NUMBERS

300+

CUSTOMERS WORLDWIDE

195

COUNTRIES COVERED

100,000+

REGULATIONS

→| complianceandrisks.com