



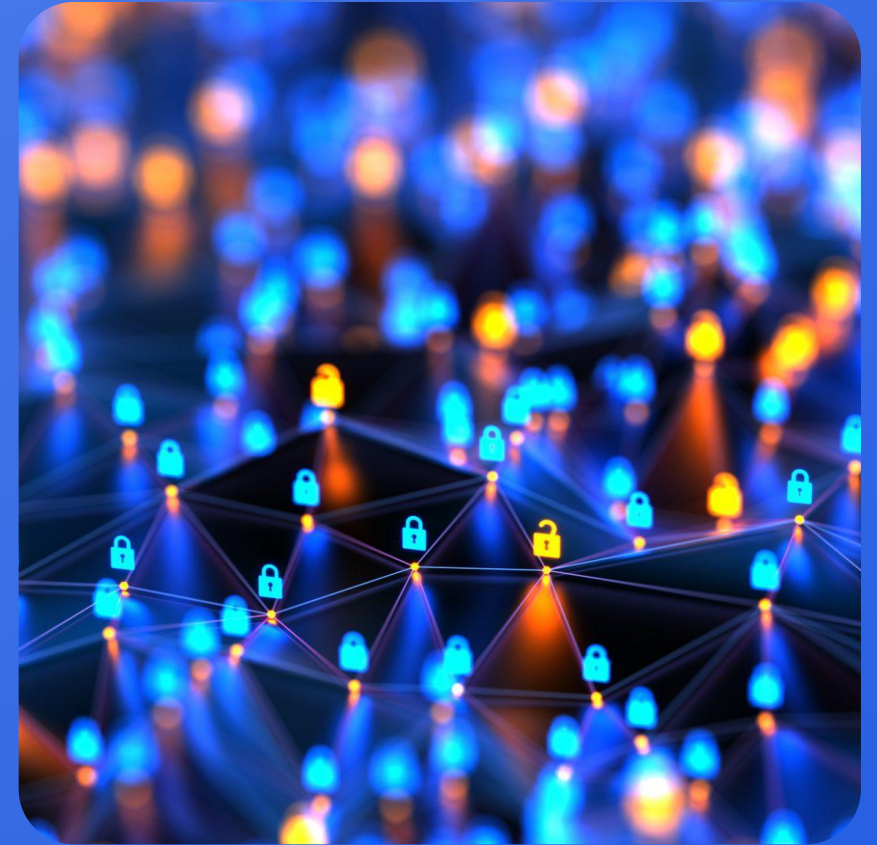
Compliance & Risks



Webinar

New Rules, New Risks: Latest Cybersecurity & Data Protection Impacts on Product Compliance

13 August, 2025



→ | complianceandrisks.com



Q&A
Session

Slides &
Webinar
Recording



Request a
Demo

Webinar Platform Tips

Meet the Team



Ashley Weeks
Senior Regulatory
Compliance Consultant,
RINA Tech UK Ltd



Orlaith Morris
Content Marketing
Manager, Compliance &
Risks

Mission Statement

**Ensure global companies have the tools
& information to build safe, sustainable,
products in a world full of change**

Trusted by the World's Leading Brands

SAMSUNG

Miele



EPSON®



FUJITSU



BELDEN

PHILIPS

logitech

XEROX®

Thermo
SCIENTIFIC



GARMIN™



Compliance & Risks



100K⁺
Regulations

195
Countries

10⁺
Industries

28
Languages

30
Global
Network
Partners

9.6k
Expert Queries
answered



WHAT WE DO

Unlocking Market Access

Keep on top of regulatory changes and their impact worldwide. Early warning alerts, impact probability, productivity workflow tools and so much more.



RINA Overview



Energy & Mobility

Energy solutions from O&G to renewables, asset integrity, product compliance, taking care of ESG impacts.



Marine

Certifications, technologies and innovative services to manage transport and pleasure vessels.

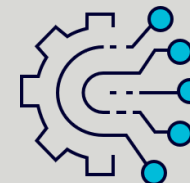


Real Estate & Infrastructure

The path to the next generation of buildings and infrastructure by ensuring their safety and efficiency.

Industry

Industry 4.0, R&D, innovation, advanced materials, full-scale testing, sustainability.



Digitalisation

Solutions to support products, people and processes on their way to excellence.



Inspection, Field & Legal

Vendor inspection, field activities and certification and compliance.



5,800 People

220+ Offices

70+ Countries

>€797m Turnover

Product Regulatory Compliance – Meet the team



Emily Tyrwhitt Jones

- Team Lead, Chemist



Ashley Weeks

- Electrical and Electronic Engineering



Charles Hlangabeza

- Environmental Resource Management



Liz Kimber

- Mechanical Engineer



Sumithra Rao

Mechanical and Product Design Engineering



Cathy Phillips

- Mechanical & Materials Engineer



Tayyaba Rizvi

- Chemist



Alan Sellers

- Electronics Engineering and Computer Science



Tony Lord

- Chemist
- Food Contact Specialist



Prerna Chaturvedi

- Environmental Engineering and Computer Science



Natalie Armstrong-Green

- Chemist

Webinar objectives



- Why cybersecurity is a regulatory priority and how jurisdictions are responding through legislation
- What is happening in the UK? – Overview of the UK PSTI Act
- What is happening in Europe? An introduction to EU CRA and the newly established RED Cybersecurity requirements
- Relationships with other union legislation (where applicable)
- How cybersecurity requirements increasingly align with data protection principles
- Are processes working?

Cyber attacks on the rise!



- In the first six months of 2024, there was a **23 %** increase in global cyber attacks, with an average of 9 serious incidents per day
- In the first half of 2024, 1,637 serious cyber attacks were counted globally.
- Attacks continued to grow, with a monthly average of 273 attacks, up from 230 in 2023 and 139 in 2019.
- Most of the attacks were concentrated in the Americas (41%) and Europe (29%), with the latter seeing a significant increase over past years.
- The escalation is accelerated by geopolitical conflicts that, increasingly, aim to destabilise digital infrastructures, exposing essential data and services to serious risks.
- The manufacturing sector has been the hardest hit, while in healthcare, attacks have increased by 83 percent since 2023 (296 incidents in six months), threatening the health data security of thousands of citizens

Real life example

Major cyber attack disrupts internet service across Europe and US

Denial of service attack from unknown culprits on domain name system company Dyn caused access to be severely restricted for users on Friday



Platforms affected by the attack included Twitter, Netflix, Reddit and Spotify. Photograph: Ross M. Horowitz/Getty Images

In 2016, cyber criminals used thousands of compromised connectable products to launch **Distributed Denial of Service** (DDOS) attacks that disrupted the services of major news and media organisations such as the BBC and Netflix, as well as leaving much of the internet inaccessible across the US east coast.

Why is cybersecurity a concern in relation to product compliance?



Why is It
Prominent?

How do Cyber-
Attacks
Happen?

Lack of
Support!

Are current products on the market cyber secure?



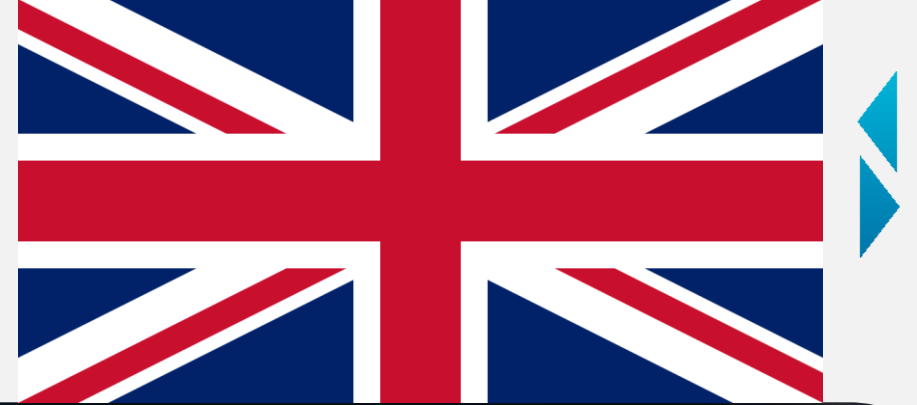
All this leads to...

More Regulations!

- Regulators are responding to the threat!
- Certain Jurisdictions are acting at different speeds
- This can lead to Regulatory divergence



UK legislation

The background of the lower half of the slide is a close-up photograph of a computer keyboard. A semi-transparent blue rectangular overlay covers the bottom portion of the image, providing a background for the title text.

THE PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE ACT (PSTI)

PSTI act and regulations

Came into effect on the 29th April 2024

Aim:

- This Regulation aims to provide baseline security requirements for IOT devices who sell to UK **consumers**

Scope:

- Products that fall within scope of PSTI are defined as “Relevant Connectable Products” (RCPs)
- **RCPs** are defined as:
 - Products which are **internet connectable**
 - Products which are **network connectable**

Internet connectable products

Internet-connectable products

- (1) In this Part “internet-connectable product” means a product that is capable of connecting to the internet.
- (2) The reference in subsection (1) to connecting to the internet is a reference to using a communication protocol that forms part of the Internet Protocol suite to send and receive data over the internet.

Internet connectable products are devices capable of sending and receiving data over the global Internet using standard protocols (e.g., TCP/IP) via Wi-Fi, Ethernet or cellular networks.



Network connectable products

Network-connectable products

- (3) In this Part “network-connectable product” means a product that—
- (a) is capable of both sending and receiving data by means of a transmission involving electrical or electromagnetic energy,
 - (b) is not an internet-connectable product, and
 - (c) meets the first connectability condition (see subsection (4)) or the second connectability condition (see subsection (5)).
- (4) A product meets the first connectability condition if it is capable of connecting directly to an internet-connectable product by means of a communication protocol that forms part of the Internet Protocol suite.
- (5) A product meets the second connectability condition if—
- (a) it is capable of connecting directly to two or more products at the same time by means of a communication protocol that does not form part of the Internet Protocol suite, and
 - (b) it is capable of connecting directly to an internet-connectable product by means of such a communication protocol (whether or not at the same time as it connects to any other product).



Does not connect directly to the internet, but
Can connect to other devices that do — either directly or as part of a local network.

First Condition

The product can connect directly to an internet-connected device using an Internet Protocol (IP)-based method.



Example:

A smart home hub that connects via Wi-Fi (IP-based) to a smart speaker which is connected to the internet.

Second Condition

The product can connect to:

Two or more other devices using a non-IP protocol (e.g. Bluetooth, Zigbee), and

At least one of those devices must be internet-connected, even indirectly



Example:

A Bluetooth fitness tracker that syncs with your phone and a smartwatch, your phone is internet-connected, so the tracker qualifies.

Excepted Connectable Products

Excepted Connectable Products (OUT OF SCOPE!)

- Products made available for supply in Northern Ireland to which relevant legislation applies (Single Market)
- Charge points for electric vehicles (Electric Vehicle (Smart Charge Points) Regulations)
- Medical devices (Medical Devices Regulation)
- Smart meter products (Subject to Relevant Energy License Conditions)
- Desktop, Laptop computers, and Tablets which do not have the capability to connect to cellular networks (unless specifically designed for children under 14 years of age)



PSTI Act and regulations

Who has to comply?

The Act sets out the duties of the **relevant persons**, in a similar way to how European Directives/Regulations lay out obligations of 'economic operators.'

- **Manufacturer** must ensure that products placed on the market have met security requirements
- **Importers** and **Distributors** also have duties placed upon them to not make available a product unless it is accompanied by a statement of compliance with proof of meeting those security requirements.

All have a duty to ensure consumers are protected!



PSTI Act and regulations

How to Comply?

- **Banning universal default and easily guessable passwords:**
Passwords must be unique per product, not based on incremental counters, nor based on publicly available information etc.
- **Publishing information on how to report security issues:**
Implement a means to manage reports of vulnerabilities. At least one point of contact to allow a person to report security issues, which must be free of charge, they must acknowledge and offer status updates until resolution has been resolved.
- **Publishing information on minimum security update periods:**
The defined support period must be published, if it changes or is extended, it shall be defined as soon as practicable.



What to expect?

- Product is accompanied by a statement of compliance as per schedule 4 of The Product Security and Telecommunications Infrastructure Regulations 2023.
- SOC should state compliance with minimum 3 security requirements, this can be achieved by complying with the conditions of schedule 2 (relevant clauses of ETSI EN 303 645)

What not to expect?

- PSTI is not legislation that requires UKCA label affixed to products.*



[Redacted]

Statement of Compliance

Product Details

Product: Mobile Phone
Model(s): [Redacted]
Variant Model(s): [Redacted]
* The symbol "" in the model name can be any alphanumeric character, '-', '/' or blank

Manufacturer

Name: [Redacted]
Registered trade name: [Redacted]
Address: [Redacted]

Declaration

This statement of compliance is prepared by Samsung. In our opinion the product above complies with the applicable security requirements in Schedule 1 of The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023.

Defined Support Period

- Defined Support Period: 7 years from the date of initial supply, 2024
- Defined End of Support Period: January 31, 2031

Reference Standard

Standard: ETSI EN 303 645
Identification Number: [Redacted]
Version: 2.1.1
Date of issue: 29.06.2020

Website for information and to report security issues <https://security.samsungmobile.com>

Signed for and on behalf of: Samsung (Authorized Representative)

<p>[Redacted] [Redacted] [Redacted] [Redacted] 01/02/2024 (Place and date of signature)</p>	<p>[Redacted] [Redacted] [Redacted] [Redacted] (Name and signature of authorized person)</p>
---	--

* This is not the address of Samsung Service Centres. Please see the address or the phone number of Samsung Service Centres in the warranty card or contact the retailer where you purchased your product.

EU Legislation



THE EU CYBER RESILIENCE ACT (CRA)

EU Cyber Resilience Act

Aim:

To fill the gaps, clarify the links, and make the existing cybersecurity legislative framework more coherent, ensuring that products with digital components, for example IoT products, are made secure throughout the supply chain and throughout their lifecycle.

Scope:

Applies to “Products with Digital Elements (**PDEs**) whose ‘intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network’”.

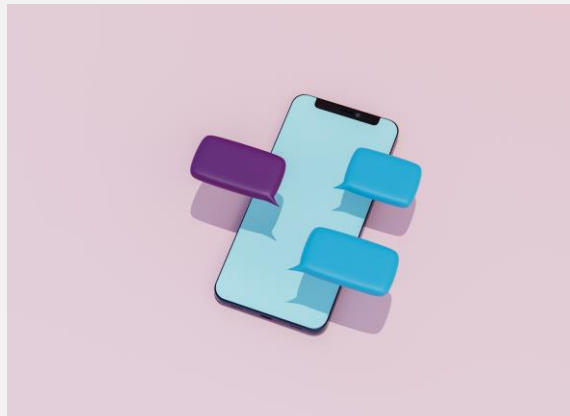
PDEs are defined as -

any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately.

PDE end devices (laptops)



PDE software (mobile apps)



Components (CPU's)



Exclusions

The Regulation proposes the following exclusions:

- **PDEs** covered by Regulation (EU) 2017/745 (Medical Devices)
- **PDEs** covered by Regulation (EU) 2017/746 (In Vitro Diagnostic Medical Devices)
- **PDEs** covered by Regulation (EU) 2019/2144 (Motor Vehicles)
- Products certified in accordance with (EU) 2018/1139 (Civil Aviation)
- Equipment that falls within scope of Directive (EU) 2014/90 (Marine Equipment)
- **PDEs** developed exclusively for national security or military purposes
- Spare parts made available to replace identical components in **PDEs**



Classification of products

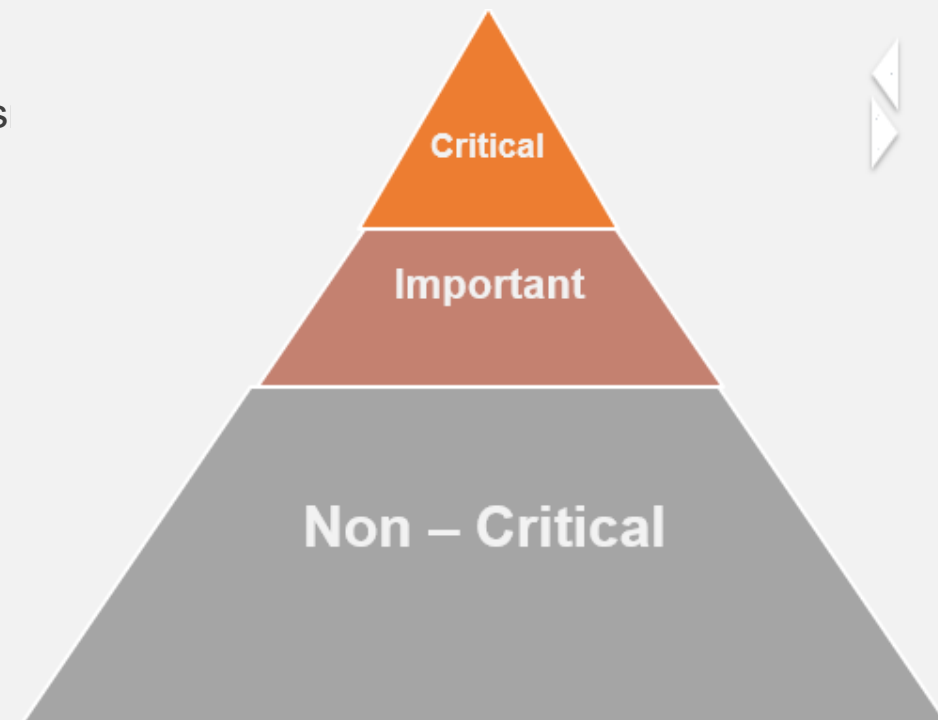
Non-Critical

Manufacturers with products in the Non- Critical category can use self-assess to demonstrate compliance with CRA essential requirements

Important Class I

PDE's that perform functions critical to the cybersecurity of other products

Manufacturers can self-assess if they apply a harmonised standard in full or European Cybersecurity Certification.



Important and Critical Category Lists will be amended over time via Delegated Acts!

Classification of products

Important Class II

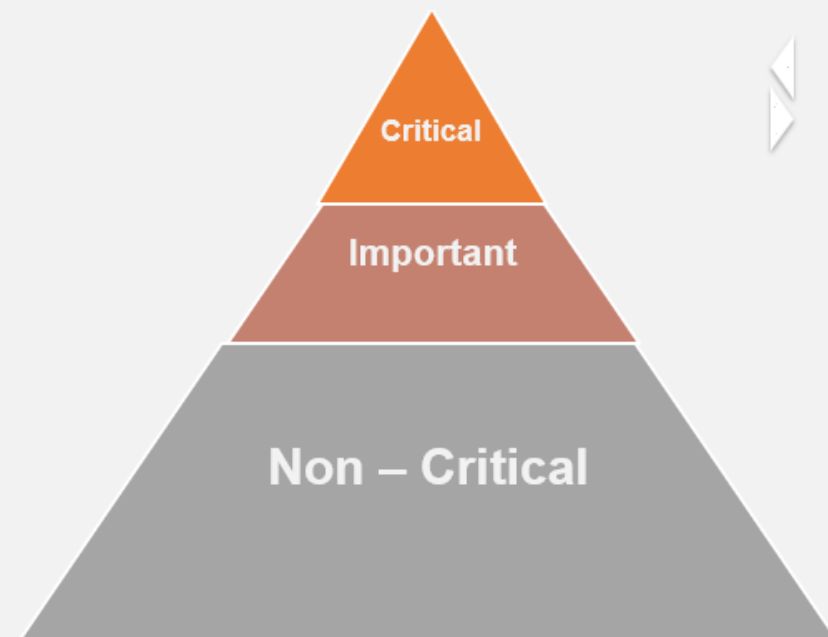
PDE's that perform a function which carries a significant risk in terms of its ability to disrupt, control or cause damage to a large number of other products

Products in the Important Class II must complete a third-party conformity assessment or use a European cybersecurity certification scheme.

Critical Class

Products that could lead to serious disruptions of critical supply chains across the internal market.

Products in the Critical Class must complete a European Common Criteria (EUC) cybersecurity certification assessment conducted by a conformity assessment body.



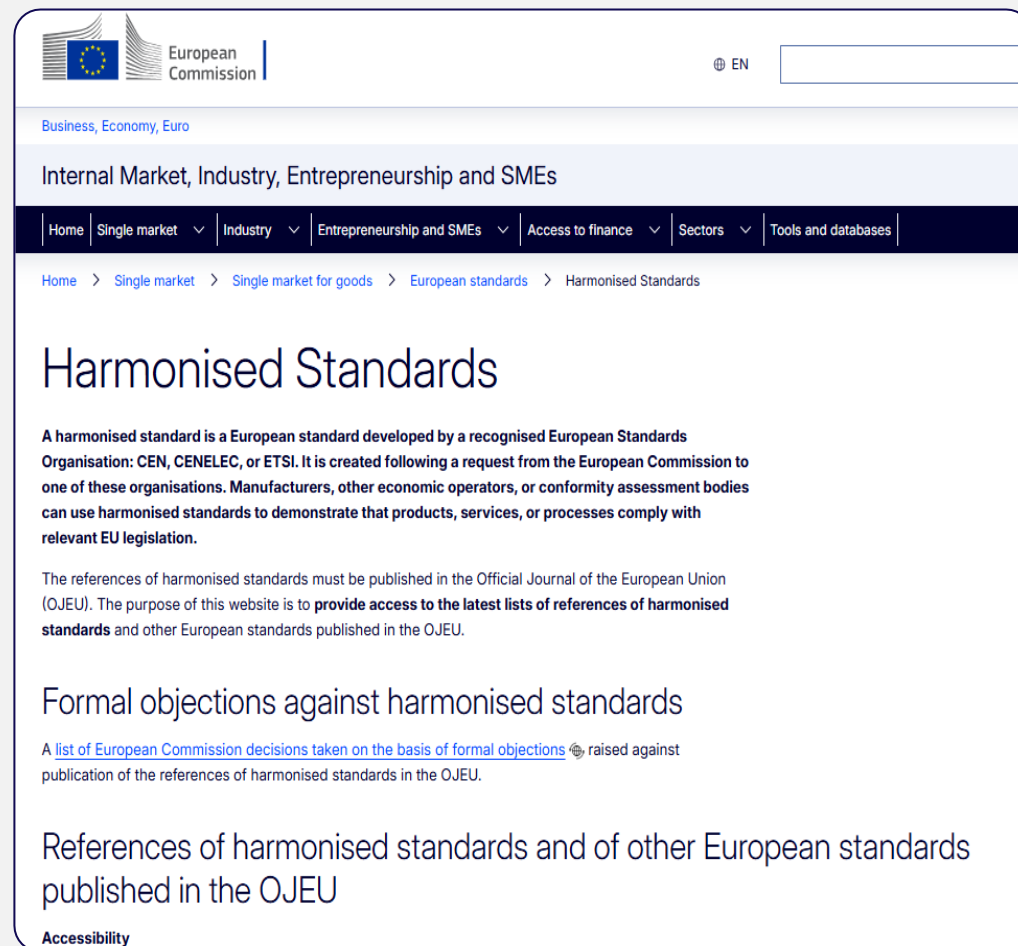
Important and Critical Category Lists will be amended over time via Delegated Acts!

Essential requirements

The CRA provides a basic set essential requirements:

Essential cybersecurity requirements in Annex I of the CRA proposal

- risk assessment during development stage
- be made available on the market without known vulnerabilities
- ensure that vulnerabilities can be addressed through security updates
- protect the confidentiality of stored data
- draw up a software bill of materials
- be designed, developed and produced to limit attack surfaces
- put in place and enforce a policy on **coordinated vulnerability disclosure**



The screenshot shows the European Commission website. The header includes the European Commission logo and the text 'European Commission'. Below the header, there is a navigation bar with links: 'Business, Economy, Euro', 'Internal Market, Industry, Entrepreneurship and SMEs', 'Home', 'Single market', 'Industry', 'Entrepreneurship and SMEs', 'Access to finance', 'Sectors', and 'Tools and databases'. The main content area is titled 'Harmonised Standards' and contains the following text:

A harmonised standard is a European standard developed by a recognised European Standards Organisation: CEN, CENELEC, or ETSI. It is created following a request from the European Commission to one of these organisations. Manufacturers, other economic operators, or conformity assessment bodies can use harmonised standards to demonstrate that products, services, or processes comply with relevant EU legislation.

The references of harmonised standards must be published in the Official Journal of the European Union (OJEU). The purpose of this website is to **provide access to the latest lists of references of harmonised standards** and other European standards published in the OJEU.

Formal objections against harmonised standards

A [list of European Commission decisions taken on the basis of formal objections](#) raised against publication of the references of harmonised standards in the OJEU.

References of harmonised standards and of other European standards published in the OJEU

Accessibility

Economic operators

Different requirements apply to economic operators that are consistent with other CE marking-type legislation

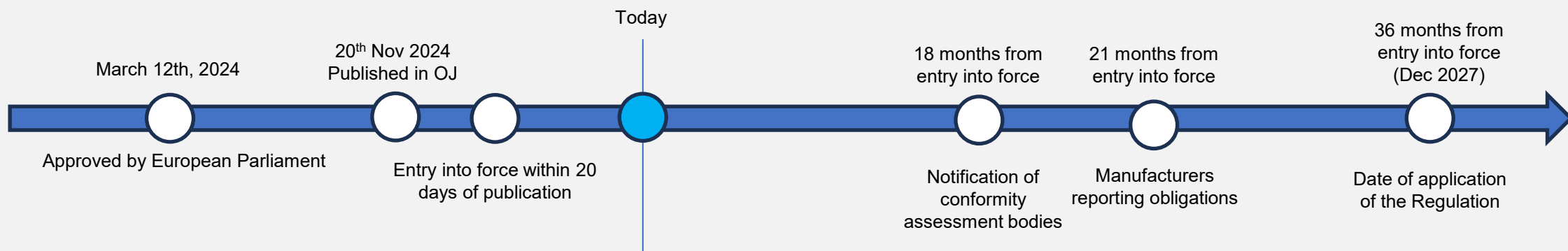
Manufacturers:

- Due diligence of 3rd party components,
- Define support periods
- Draw up technical documentation,
- Provide information and instructions,
- Supply a DOC can be simplified (similar to RED),
- Affix CE marking,
- Reporting known vulnerabilities (which will be established by ENISA)

Importers and Distributors:

- General Due Diligence obligations
- Ensure essential requirements have been met.
- Ensure current conformity assessment procedure has been followed
- Inform manufacturers of vulnerabilities
- **Importers** shall also provide their details on packaging or in an accompanying product with digital elements

EU CRA timeline



Upon the CRA Act entering into force, Guidance from the EU Commission is expected in relation to the scope of the CRA.

Find more information [here](#).

Penalties

Penalties for infringements by economic operators lie with individual Member States. However, the regulation sets onerous administrative fines starting from €5 million and can result in much larger fines.

Relationship with Union Legislation

NIS2 Directive (Network and Information systems)

- Framework provides a common level of cybersecurity in 18 critical and important sectors (energy, transport, healthcare, finance, water management etc). Therefore, more products compliant with the EU CRA would facilitate compliance by the entities in the scope of the NIS2 Directive and would strengthen the security of the entire supply chain.

The EU Cybersecurity Act

- The EU Cybersecurity Act introduces an EU-wide cybersecurity certification scheme (Document will include Scope, requirements, type of evaluation). If your product falls within scope, can be used to comply with requirements of EU CRA.



Relationship with Union Legislation

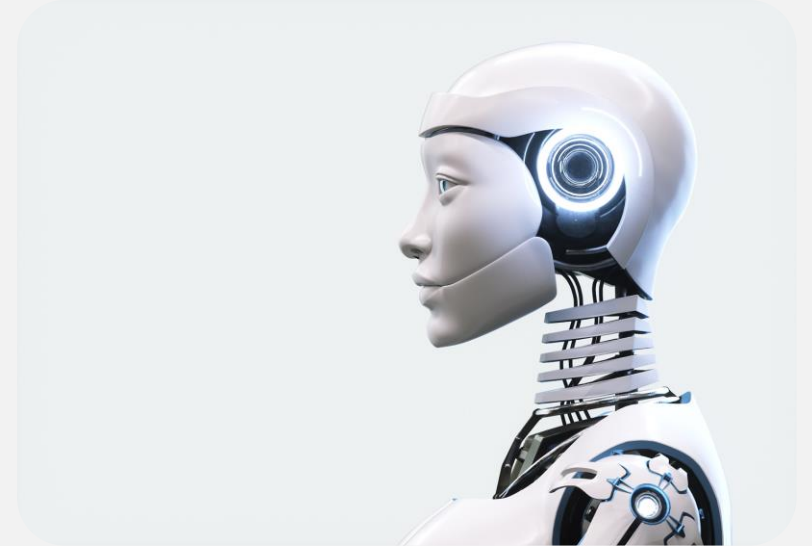
EU AI Act

- AI systems within scope of the EU AI Act will have to meet Cybersecurity requirements. Comply with CRA and you shall be deemed compliant against the cybersecurity requirements set out in the AI Regulation.

New Machinery Regulation

- No official synergy between the legislations, synergies expected to take place at standards level to deal with state-of-the-art machinery.

And...



EU Legislation



THE RADIO EQUIPMENT DIRECTIVE (RED) CYBERSECURITY REQUIREMENTS

(RED Delegated Regulation 2022/30/EU)

RED Delegated Regulation 2022/30/EU

Same Scope, Enhanced Security!

Entered into force 1st August 2025

- Retains the same scope as 2014/53/EU (RED) and conformity procedures
- Adds mandatory cybersecurity measures to strengthen device resilience

3 new essential requirements under article 3 of RED Directive 2014/53/EU

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



RED Delegated Regulation 2022/30/EU

Example of something within scope

- A Wi-Fi or LTE module clearly connects to the internet, so it triggers the Delegated Regulation's cybersecurity obligations.



Example of something not within scope

- A simple garage door opener using RF signals is in scope of RED but does not connect to the internet, so the new cybersecurity rules don't apply.



How to comply? (EN 18031 series)

EN 18031-1,2 & 3 (Article 3.3 (d) Network Protection, (e) Personal Data & Privacy Protection & Article 3.3 (f) – Fraud Prevention :

2014/53/EU	CEN	EN 18031-1:2024	Common security requirements for radio equipment - Part 1: Internet connected radio equipment
------------	-----	-----------------	---

Restriction 1!

Devices that allow blank or unchangeable default passwords under EN 18031-1:2024 (as per Clauses 6.2.5.1 and 6.2.5.2) lose the presumption of conformity with RED Article 3(3)(d) and must undergo a full Notified Body assessment.

Device Behaviour	EN 18031-1 Outcome	RED 3(3)(d) Presumption	Conformity Assessment Procedure
Ships with a unique default password and forces the user to change it	Compliant with Clauses 6.2.5.1 & 6.2.5.2	Presumption of conformity can be used	Self-declare via harmonised standard (Module A)
Ships with a blank or unchangeable default password, or skips password setup	Non-compliant with Clauses 6.2.5.1/6.2.5.2	Presumption of conformity lost	Notified Body assessment required
No password login but uses certificate-based or token-based authentication (acceptable alternatives)	Compliant if the alternative meets EN 18031-1 authentication requirements	Presumption of conformity can be used	Self-declare via harmonised standard (Module A)

How to Comply? (EN 18031 series)

EN 18031-2 (Article 3.3 (e) – Personal Data & Privacy Protection):

2014/53/EU	CEN	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
------------	-----	-----------------	---

Restriction 2!

For certain child-oriented radio devices covered by clauses 6.1.3–6.1.6, you only comply with the privacy requirement in Article 3(3)(e) if you build in specific real parental or guardian controls detailed within these clauses.

Device Behaviour	EN 18031-2 Outcome	RED 3(3)(e) Presumption	Conformity Assessment Procedure
Implements parental access control as required by Clauses 6.1.3–6.1.6	Compliant with Clauses 6.1.3–6.1.6	Presumption of conformity can be used	Self-declare via harmonised standard (Module A)
Omits, bypasses or provides non-functional parental controls	Non-compliant with Clauses 6.1.3–6.1.6	Presumption of conformity lost	Notified Body assessment required
Not a toy, child wearable or childcare gadget	Harmonised (clauses not triggered)	Presumption of conformity can be used	Self-declare via harmonised standard (Module A)

How to Comply? (EN 18031 series)



EN 18031-3 (Article 3.3 (f) – Fraud Prevention):

2014/53/EU	CEN	EN 18031-3:2024	Common security requirements for radio equipment - Part 3: Internet connected radio equipment processing virtual money or monetary value
------------	-----	-----------------	--

Restriction 3!

EN 18031-3 may be used for presumption of conformity with Article 3(3)(f) of the RED Directive only where Clause 6.2.3.4 does not apply. If Clause 6.2.3.4 does apply, a Notified Body must be involved, since that clause alone cannot satisfy all relevant cybersecurity requirements

Device Behaviour	EN 18031-3 Outcome	RED 3(3)(f) Presumption	Conformity Assessment Procedure
Device has no update capability	Harmonised	Retained	Self-declaration via EN 18031-3
Device supports any update mechanism (Clause 6.2.3.4 applies)	Not harmonised	Lost	Notified Body assessment

Data protection



CYBERSECURITY LEGISLATION AND DATA PROTECTION PRINCIPLES

Linking cybersecurity legislation and general Data Protection Law

Common Goal:

Both cybersecurity legislation (like PSTI, CRA, RED Delegated Regulation) and data protection laws (e.g., GDPR/UK GDPR) aim to **protect individuals' personal data** and **ensure privacy** in an increasingly connected world.

How They Interlink:

Cybersecurity laws mandate secure product design to prevent unauthorised access and data breaches, while data protection laws require lawful handling and security of personal data. Compliance with cybersecurity standards supports meeting core data protection principles like integrity, confidentiality, and accountability.

Examples of Interlink:

- **RED Delegated Regulation's** focus on radio equipment processing personal data supports GDPR's requirement for *secure processing*.
- **ETSI EN 303 645**, referenced in PSTI, includes privacy controls that align with GDPR's privacy-by-design principle.
- The **EU CRA** aims to ensure secure products, reducing risks that lead to data breaches subject to GDPR enforcement.

Linking cybersecurity legislation and general Data Protection Law



Legislation / Regulation	Direct Reference to Data Protection?	Relevant Clauses / Articles	Relationship with Data Protection Laws (e.g., GDPR/UK GDPR)
UK PSTI Regulations	No	Minimum Security Requirements (do not explicitly reference EN 303 645 privacy clauses)	Focuses mainly on cybersecurity and device security; while EN 303 645 includes privacy provisions, PSTI's scope is primarily security-related. Security controls indirectly support personal data protection by reducing risk of breaches, but data protection is a separate compliance area.
EU Cyber Resilience Act (CRA)	Yes	Annex I Essential Requirements (e) – confidentiality of personal data (f) – integrity of personal data (g) – data minimisation	Aims to protect personal data by requiring secure digital products. While no standalone data protection clause, the CRA integrates data protection through security obligations aligned with GDPR principles.
RED Delegated Regulation (EU) 2022/30	Yes	Article 3(3)(e) — cybersecurity for processing personal and traffic data	Links cybersecurity obligations directly to personal data processing in radio equipment, ensuring compliance with data protection and privacy requirements alongside RED.

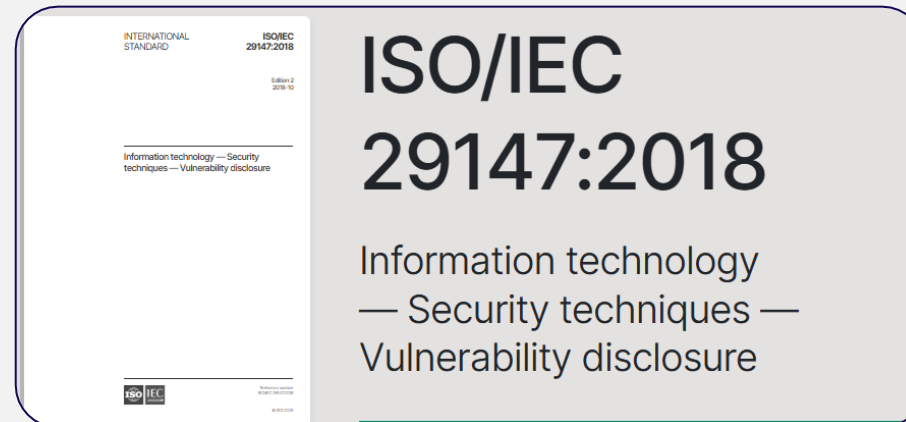
Vulnerability Disclosure Policies

The background of the slide features a close-up, slightly blurred image of a computer keyboard. A semi-transparent blue rectangular overlay covers the lower half of the image, providing a background for the text.

ARE PROCESSES WORKING?

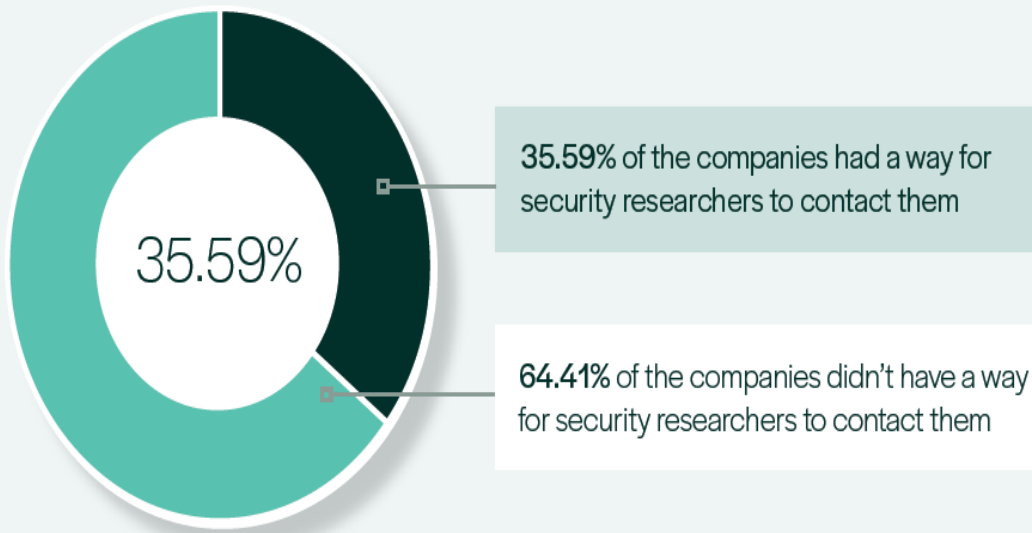
What is Vulnerability Disclosure?

- (ENISA) defines vulnerability disclosure as “the process of identifying, reporting and patching weaknesses of software, hardware or services that can be exploited
- The standardised best practice for vulnerability disclosure is called ‘Coordinated Vulnerability Disclosure’ or CVD
- In this process the researcher contacts the company, the report is acknowledged by the company within a certain period (usually 24-48 hours) and then the company sets about investigating and addressing the vulnerability reported
- Because all the reports are security related, it is likely that a swift resolution would be necessary – it is normally expected that reports are fixed in products within 30-90 days.
- Usually resolved with a software update but if it’s more serious it may require a hardware fix



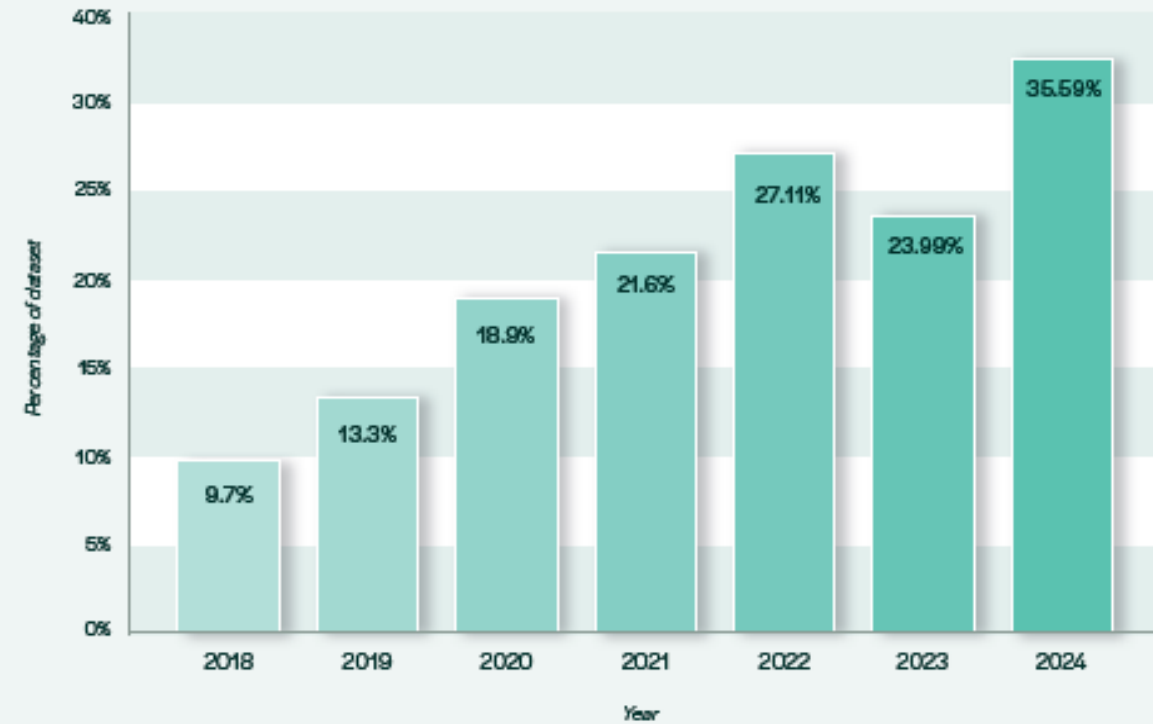
The state of Vulnerability Disclosure Policy usage in global consumer IoT

The Headline Figure



Vulnerability Disclosure in Practice Trend

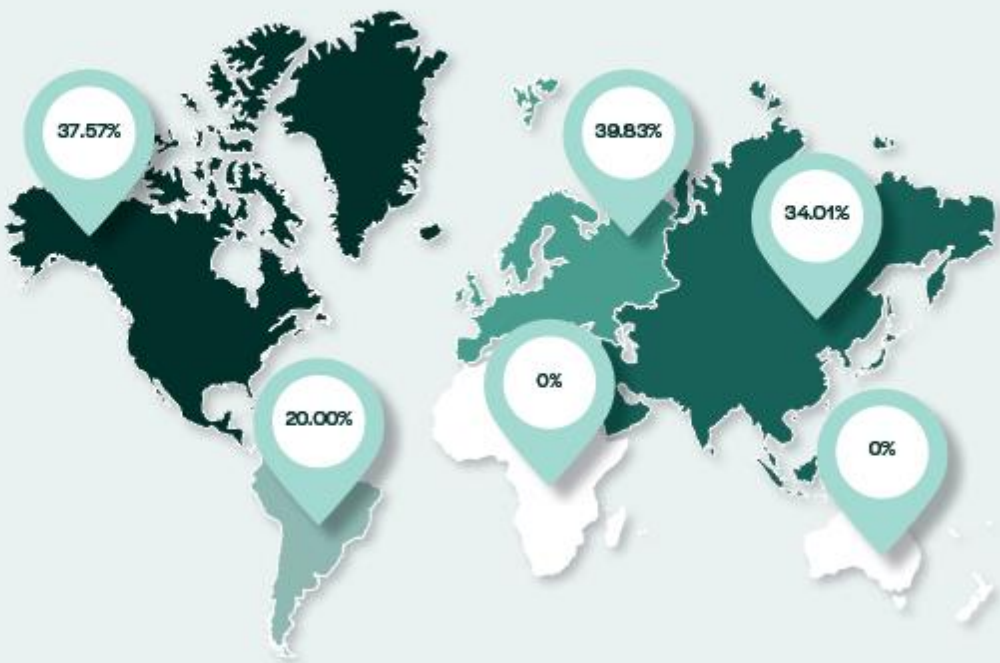
Figure 2



The state of Vulnerability Disclosure Policy usage in global consumer IoT



Manufacturer adoption of vulnerability disclosure across the world



Region / Country (Number of Retailers)	Retailers	Stocked Manufacturers Using Vulnerability Disclosure 2023	Stocked Manufacturers Using Vulnerability Disclosure 2024
European Union (5)	CDiscount, France	5/12 (41.67%)	6/12 (50.00%)
	El Corte Ingles, Spain	12/17 (70.59%)	12/17 (70.59%)
	EPrice, Italy	5/10 (50%)	6/11 (54.55%)
	Media Markt, Germany	7/8 (87.5%)	8/10 (80.00%)
	Otto, Germany	9/20 (45%)	11/20 (55.00%)
United Kingdom (3)	Amazon UK	3/14 (21.43%)	7/15 (46.67%)
	Currys	11/17 (64.71%)	10/15 (66.67%)
	John Lewis	9/10 (90%)	14/15 (93.33%)
United States of America (3)	Best Buy	8/18 (44.44%)	13/23 (56.52%)
	Target	8/10 (80%)	8/12 (66.67%)
	Walmart	6/30 (20%)	8/29 (27.59%)

The state of Vulnerability Disclosure Policy usage in global consumer IoT

Positives

- Upward trend of Vulnerability Disclosure Policies.
- UK retailers appear to be performing well (90% in some cases).
- Legislation appears to be driving more compliance.

Negatives

- Hundreds of companies within the report, still have no vulnerability disclosure policies.
- The report argues it's industry best practice and has been standardised for years so there should be no real excuse for not adopting in.
- UK legislation is now in force!
That's potentially lots of products that are simply on the market and non-compliant!

How can RINA Help?



- Provide technical training and high-level briefings
- Assess what cybersecurity regulatory requirements apply to your products and your business
- Assess compliance versus standards clause by clause
- Assess the adequacy of your due diligence efforts
- Assist with Risk Assessments
- Review Technical Files / Declaration of Conformity's / Statement of Compliance
- Assess Vulnerability Disclosure Policies



For more info:



**Thank you for
your attention**

Ashley Weeks
Senior Consultant - RINA
ashley.weeks@rina.org

Questions?



Thank You!



Ashley Weeks
Senior Regulatory
Compliance Consultant,
RINA Tech UK Ltd



Orlaith Morris
Content Marketing
Manager, Compliance &
Risks

