element

WHITEPAPER

CYBER SECURITY: RED, PSTI, AND CRA

UNDERSTANDING MANUFACTURERS' OBLIGATIONS WITH REGARD TO PRODUCT CYBER SECURITY

CONTENTS

element

CYBER SECURITY: RED, PSTI, AND CRA

Foreword from the Authors

Many of us will be familiar with the concept of cyber security, even if for no other reason than being told by our IT teams to follow best practice such as having unique passwords, not leaving workstations unlocked, and being cautious when clicking suspicious email links. But this guidance applies to our individual behaviours and our company policies and practices, and doesn't necessarily mean that the products we use (or manufacture) are secure.

With that in mind, several pieces of legislation specifically aimed at product cyber security are being introduced to address this topic. Therefore when we make reference to "cyber security" in this paper, what we really mean is "product cyber security of electrical and electronic equipment", but that's quite a mouthful.

We have also pitched this document assuming some prior knowledge on the CE marking and UKCA marking processes, test standards, and role of Notified Bodies etc. Other whitepapers and articles are available as refreshers on those topics if required at our resource hub (element.com/nucleus).

Michael Derby
Technical Director - Regulatory Approvals

Michael Derby has been in the product development and approvals business for more than 35 years. His present area of expertise is helping manufacturers get radio equipment onto the market.

As a Technical Director in Element's Connected Technology & Mobility group, Michael provides support on all topics related to radio equipment tests, certification, and authorization. He is responsible for new initiatives and growth within Element, identifying new opportunities, finding solutions, setting up new services, and training staff.

Alex Toohie
Technical Solution Manager

Alex Toohie has been working in regulatory compliance for more than a decade, both within Element's Connected Technology & Mobility group and in industry as Compliance Manager for a global leader in wireless intruder and fire alarm systems.

As Element's Technical Solution Manager, Alex draws on a wealth of experience in UKCA and CE marking (covering RED, EMCD, CPR, ATEXD, RoHSD, etc.), FCC and ISED, as well as the evolving global product cyber security requirements, to help manufacturers find the most effective and cost-efficient certification paths for complex and varied radio equipment.


57 bpm
200
150
100
50
00:00
06:00
12:00
18:00
24:00
101
49
Sessiz -- bpm

INTRODUCTION TO CYBER SECURITY LEGISLATION

CYBER SECURITY LEGISLATION

This paper will discuss three different pieces of cyber security legislation which are being introduced aiming to cover a multitude of topics, each of which is related to a known cyberattack methodology or a potential security vulnerability.

These include:

- Ensuring products do not have known vulnerabilities when they are made available on the market;
- Ensuring products are secure by default, and having the option to revert the product to this secure default state;
- Providing a mechanism for updating or making products secure if a vulnerability becomes known;
- Ensuring products are designed and manufactured with appropriate access control and authentication mechanisms to protect against unauthorised or malicious access;
- Ensuring sensitive information processed by the products is stored and communicated securely, including the use of appropriate cryptography;
- Processing data only where required for the equipment functionality, not gathering or storing data unnecessarily, and providing users with the ability to permanently delete information when no longer required;
- Minimising the attack surfaces on a product, including disabling or giving the user the ability to disable interfaces, especially networked or wireless interfaces, which are not essential for device functionality;
- Providing users with clear paths to report vulnerabilities as they are discovered, and committing to addressing these vulnerabilities, providing updates where needed, and sharing the information about potential vulnerabilities with affected third parties.

By implementing the measures above in their products, manufacturers are reducing the likelihood and severity of cyberattacks involving their products. Attacks such as:

- Networked devices being used as point-of-entry to secure networks to steal information;
- IoT devices being used to assemble of a botnet of devices for distributed denial-of-service attacks;
- Security cameras being accessed and used to assist criminal activity such as burglary;
- Connected smart devices being used to steal personally identifiable information or financial data, or to monitor location data.

Various pieces of legislation are being introduced to address the topics described above.

The UK published the Product Security and Telecommunications Infrastructure Act ("PSTI Act") in 2022, and the accompanying Product Security and Telecommunications Infrastructure Regulations ("PSTI Regulations") in 2024 – together these two pieces of legislation are known as the "PSTI Regime".

In 2021 the EU adopted Delegated Regulation (EU) 2022/30 which will enact three essential requirements under the Radio Equipment Directive 2014/53/EU ("RED"), coming into force from August 1st, 2025, a year after the initial planned date of August 1st, 2024.

The EU have also introduced the Cyber Resilience Act ("CRA", officially Regulation (EU) 2024/2847), which will bring in mandatory reporting obligations on manufacturers from September 11th, 2026, and will come into full force December 11th, 2027.

Each of these pieces of legislation has a different scope, and so the first question many manufacturers have to answer is which legislation must their products meet. The decision tree on page 7 aims to simplify this step, and the specific applicability is discussed in each of the following sections of this paper.

UNDERSTANDING THE CYBER SECURITY LEGISLATION

UK PSTI REGIME

The PSTI Regime was the first piece of legislation introduced globally that brought in specific mandatory cyber security requirements for a broad range of products. The Act was signed into law in September 2023, before coming into force in April 2024. Compared to most new pieces of product legislation this is a very short timeline.

The requirements under the PSTI Regime were, however, relatively easy to comply with. There is fundamentally only one technical requirement under the PSTI Regime, and that is that passwords must be unique per product or be capable of being defined by the user.

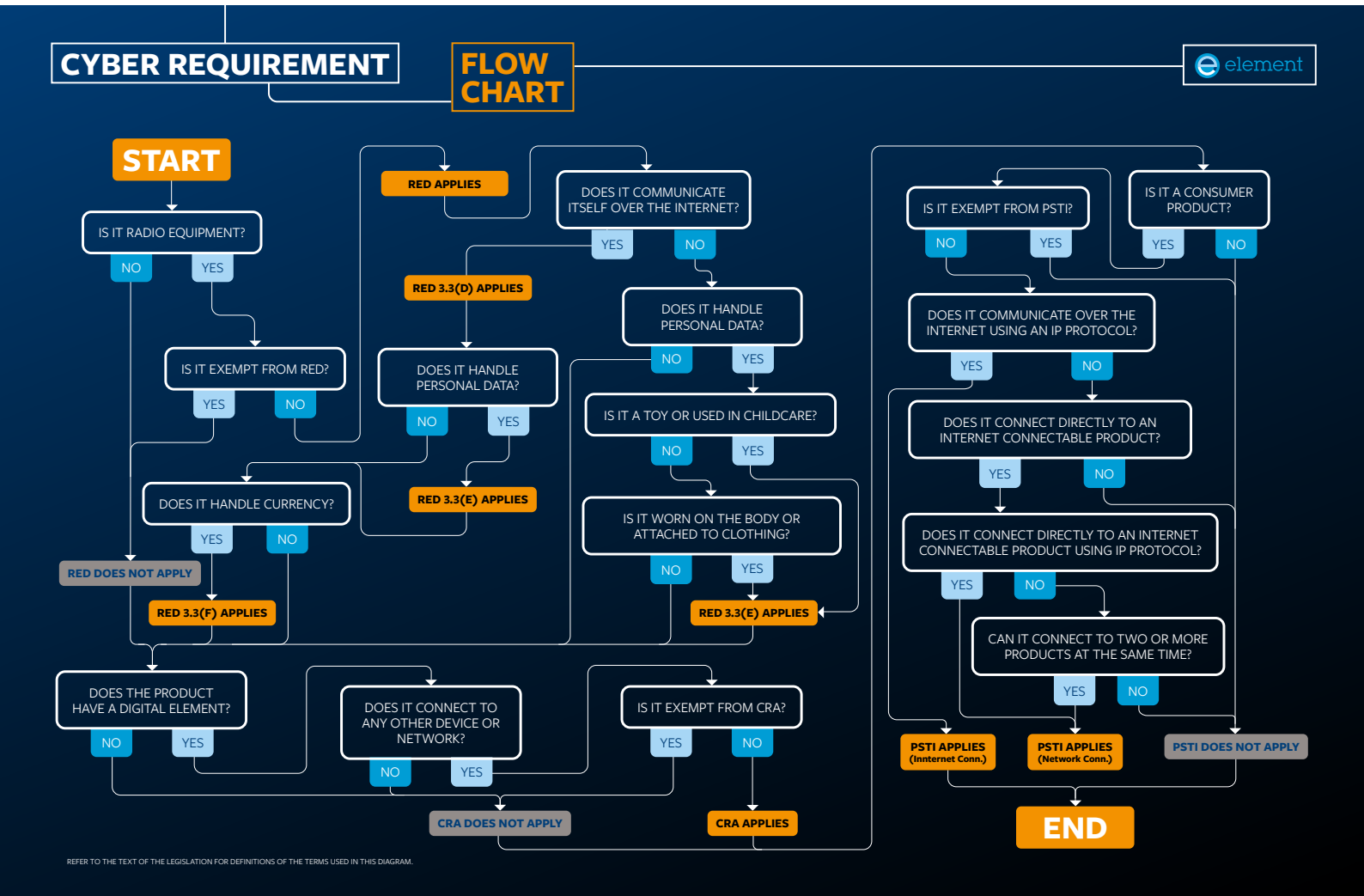
The other three requirements under the PSTI Regime are that the manufacturer must:

- Provide information on how to report security issues about their product, and must also provide information on the timescales within which updates can be expected by person making the report;
- Publish information on the minimum security update period they support for the product, and they must not shorten this period after publication;
- Provide a statement of compliance with the product.

STANDARDS

The PSTI Act refers out to EN 303 645, published by ETSI, which is one of the first widely-available standards aimed at covering horizontal cyber security requirements for a range of product types. Specifically, it refers to provisions 5.1-1, 5.1-2, 5.2-1, and 5.3-13 of that standard, which cover the same points above (save for the statement of compliance which is not in the standard).

EN 303 645 is a freely-available standard, as is the complementary technical specification, TS 103 701, which provides testing methodologies for the provisions listed in EN 303 645.



UNDERSTANDING THE CYBER SECURITY LEGISLATION

SCOPE

The PSTI Regime applies only to connectable consumer products being placed on the UK market, and defines this as covering any products which are:

- Internet-connectable, defined as using a communication protocol that forms part of the Internet Protocol suite to send and receive data over the internet; or
- Network-connectable, which is further defined as either:
    - Able to connect to an internet-connectable product using a communication protocol that forms part of the Internet Protocol suite; or
    - Able to connect to an internet-connectable product using any other communication protocol and can connect to two or more products simultaneously.

The decision tree on page 7 helps with this determination. The text in sections 4, 5, and 54 of the PSTI Act should be consulted if there is any ambiguity.

PLACING ON THE MARKET

Similarly to CE marking or UKCA Marking, the requirements apply to each individual unit, not a product type or a production run. Products which are placed on the market after April 29th, 2024 must meet the applicable requirements at that point in time, regardless of whether that same product type was available before that date or not.

STATEMENT OF COMPLIANCE

The PSTI Regime is unrelated to CE or UKCA marking, and there are no additional product markings required. The product must be accompanied by a signed statement of compliance which should include similar information to the UKCA or CE DoC:

- Identifying information for the product;
- Name and address of the manufacturer or authorised representative;
- A declaration that the statement of compliance is prepared by or on behalf of the manufacturer;
- A declaration that the product meets the technical requirements;
- The support period of the product;
- Reference to any standards used in the assessment;
- Name, function, date, and place of signature.

It is permissible for the UKCA DoC and the PSTI Regime statement of compliance to be on the same document.

EU RADIO EQUIPMENT DIRECTIVE

Since the RED was first published, Article 3(3) has contained additional essential requirements that could apply to specific equipment categories. These nine additional essential requirements are often imagined as a bank of switches, all of which were switched off to begin with, and which could be switched on (enacted) by the European Commission ("EC") for specific equipment categories. Article 3(3)(g) has already been enacted for various categories of equipment relating to radiolocation beacons and smartphones, but the key part for the topic of cyber security is that Articles 3(3)(d), 3(3)(e), and 3(3)(f) have been enacted by Delegated Regulation (EU) 2022/30, and from August 1st, 2025 these requirements will become mandatory.

The three requirements aim to address different topics, and apply to different categories of equipment:

- Article 3(3)(d) requires that products protect the network from harm. It aims for example to ensure that internet-connected products are not compromised in ways that could allow for botnets to be assembled, or for a single weak device to act as the point of entry for malicious actors into a network. This requirement applies only to internet-connected radio equipment.
- Article 3(3)(e) requires that products protect data and privacy. It aims for example to prevent malicious actors from gaining access to personally-identifiable data, especially in instances of special categories of data, or where that data may pertain to children. This requirement only applies to radio equipment which processes personal data, traffic data, or location data and which is either internet-connected, body-worn or carried, used by children, or is a toy.
- Article 3(3)(f) requires that products protect from fraud. It aims for example to ensure that increased protection is in place when financial assets, money, or virtual currency is being processed to prevent malicious actors from being able to access or alter such assets. This requirement only applies to internet-connected radio equipment which processes financial assets.

The decision tree on page 7 aims to help with the determination of which essential requirements apply to which product types. The text in Article 1 of Delegated Regulation (EU) 2022/30 should be consulted if there is any ambiguity.

There is some ambiguity over what "internet-connected" means in the context of the RED Delegated Regulation. The actual text defines internet-connected radio equipment as equipment which "can communicate itself over the internet". In the absence of an updated RED Guide, we can look to Recital (5) of the preamble to the Delegated Regulation to expand on this, which states that such equipment "operates protocols necessary to exchange data with the internet". Despite a lack of official guidance, the consensus in the industry is that this means one end of an IP link, i.e. a device with IP address 12.34.56.789 which attempts to communicate with some remote device with IP address 98.76.54.321, for example.

UNDERSTANDING THE CYBER SECURITY LEGISLATION

The RED Delegated Regulation further explains that this connection need not be direct, i.e. equipment can still be in scope of this requirement if it connects to the internet via some other equipment.

STANDARDS

Three standards have been cited in the Official Journal of the EU (OJEU) to address these new requirements, but each of these has been listed with restrictions:

- EN 18031-1:2024 addresses Article 3(3)(d) with the following restrictions:
    - If clause 6.2.5.1 or 6.2.5.2 of the standard is applicable to the product (which relate to user passwords), and if the user of the product is permitted not to set and use a password, the standard does not confer presumption of conformity with the RED essential requirements.
- EN 18031-2:2024 addresses Article 3(3)(e) with the following restrictions:
    - If clause 6.2.5.1 or 6.2.5.2 of the standard is applicable to the product (which relate to user passwords), and if the user of the product is permitted not to set and use a password, the standard does not confer presumption of conformity with the RED essential requirements.
    - If clause 6.1.3.4.2, 6.1.4.4.2, 6.1.5.4.2, or 6.1.6.4.2 is applicable to the product (which relate to parental or guardian control for equipment used by children), and if parental or guardian control is not ensured on the product, the standard does not confer presumption of conformity with the RED essential requirements.
- EN 18031-3:2024 addresses Article 3(3)(f) with the following restrictions:
    - If clause 6.2.5.1 or 6.2.5.2 of the standard is applicable to the product (which relate to user passwords), and if the user of the product is permitted not to set and use a password, the standard does not confer presumption of conformity with the RED essential requirements.
    - If clause 6.3.2.4 is applicable to the product (which relates to secure update mechanisms), the standard does not confer presumption of conformity with the RED essential requirements.

Additionally, all three have been cited with a note that sections named 'rationale' and 'guidance' are not to be considered as normative and do not confer a presumption of conformity with the RED essential requirements.

CONFORMITY ASSESSMENT PROCEDURES

The implication of the above restrictions for manufacturers of affected radio equipment is that their choice of conformity assessment procedure ("CAP") is limited if their product falls within one of these restrictions.

Referring to RED Article 17, three CAPs are in general available to manufacturers of radio equipment:

- Internal Production Control (the traditional route to compliance based on a declaration of conformity and not requiring a Notified Body);
- EU-Type Examination (by a Notified Body) followed by Conformity to Type (similar to Internal Production Control);
- Full Quality Assurance (by a Notified Body).

As can be seen, only the Internal Production Control route can be achieved without a Notified Body.

RED Article 17 clarifies that any of these three CAPs can be used when assessing a product for conformity with the essential requirements in Articles 3(1) or 3(4) (which cover EMC, safety, and common charger requirements), but that for Articles 3(2) (radio spectrum usage) and 3(3) (including the cyber security requirements), the choice of CAP depends on the application of Harmonised Standards that have been cited in the OJEU:

- If the manufacturer has fully applied Harmonised Standards that have been cited in the OJEU, they may use any of the three CAPs above.
- If the manufacturer has not fully applied Harmonised Standards that have been cited in the OJEU (including cases in which no such standard exists, or in which relevant restrictions exist), they are no longer permitted to use Internal Production Control and must follow EU-Type Examination followed by Conformity to Type or Full Quality Assurance, both of which will require a Notified Body.

Therefore, products which fall under these restrictions must be reviewed by a Notified Body before being placed on the market. It is worth noting that until August 1st, 2025, Notified Bodies may not issue an EU-Type Examination Certificate for the cyber security requirements, as no such requirements are yet in force. Practically, many Notified Bodies will issue draft certificates, and will issue final copies on August 1st.

It is also worth noting that the EC have published guidance cautioning manufacturers to be wary of certification bodies, including Notified Bodies, offering to issue "voluntary" certificates which are not official EU-Type Examination Certificates. Under EU law, voluntary or other additional certificates are not a recognised means to prove compliance. Consequently, such certificates have no value in case of checks by market surveillance authorities or customs, and can create the impression that a product is in conformity with the relevant legislation when it may not be. The CE marking must only be affixed after performing the proper CAP as appropriate to the product.

UNDERSTANDING THE CYBER SECURITY LEGISLATION

RISK ASSESSMENT

The RED, like other EU Directives, requires the manufacturer to perform an adequate analysis and assessment of the risks, with regard to compliance. This risk assessment must be available for the manufacturer to show to a market surveillance authority or to a Notified Body if requested.

The risk assessment is an essential document and a very important part of the manufacturer's technical documentation, and would typically be the first document the manufacturer opens and the last one they close when CE marking a product. It is not expected that the risk assessment is a document created at the end of the compliance process.

There is no template or clear list of what must appear in the manufacturer's risk assessment. Manufacturers will all have their own approach to this, for their own unique products. Further guidance on risk assessment is provided in other whitepapers.

https://www.element.com/nucleus/2017/what-is-a-radio-risk-analysis

PLACING ON THE MARKET

As with all CE marking directives and regulations, these new RED requirements apply at the point a product is placed on the market. That should be read as meaning each individual unit, not a product type or a production run. Products which are placed on the market from August 1st, 2025 must meet the applicable requirements at that point in time, regardless of whether that same product type was available before that date or not.

DECLARATION OF CONFORMITY AND CE MARKING

There are no additional product marking requirements, however the declaration of conformity (DoC) should be updated to reference the standards used in assessing the products against these requirements, and, if the DoC lists the essential requirements (which is not mandatory) then this should be updated to reflect the relevant 3(3) requirement(s) also. If an EU-Type Examination Certificate has been issued by a Notified Body, this should be listed on the DoC. The new DoC will need to be signed and dated at that point.

UNDERSTANDING THE CYBER SECURITY LEGISLATION

EU CYBER RESILIENCE ACT

The CRA entered into force in 2024 and will bring in mandatory reporting obligations on manufacturers from September 11th, 2026, with all other obligations applying from December 11th, 2027.

The scope of the CRA is very wide-reaching, applying to any products with digital elements which include a direct or indirect logical or physical data connection to any other device or network (save for some excepted product types). The decision tree on page 7 aims to help with determining which products are in scope, and the text in Article 2 of Regulation (EU) 2024/2847 should be consulted if there is any ambiguity.

It is widely expected that, once the CRA requirements become applicable, the RED requirements may be repealed, to avoid duplication of requirements between the two pieces of legislation.

IMPORTANT AND CRITICAL PRODUCTS

The CRA applies to all products with digital elements which include a direct or indirect logical or physical data connection to any other device or network, but adds additional requirements for products classified as "important" or "critical". Annexes III and IV list these product types.

STANDARDS AND SPECIFICATIONS

At the point of writing this article, no standards are yet published to address any aspects of the CRA specifically. In February 2025, the EC published a standardisation request to the standards writing bodies ETSI, CENELEC, and CEN requesting that 41 standards are created to address the CRA requirements. The expectation is this will include:

- 1 horizontal standard on vulnerability reporting;
- 14 horizontal standards on security requirements applicable to all product types;
- 26 vertical standards addressing specific requirements:
    - 19 standards for Class I important product types covered in CRA Annex III Part I;
    - 4 standards for Class II important product types covered in CRA Annex III Part II;
    - 3 standards for critical product types covered in CRA Annex IV.

Once these standards are published, the expectation is that they will be cited in the OJEU as harmonised standards. This position may well change, depending on the EC's review of the standards, and they may well be cited with restrictions, or not cited at all.

The EC is also empowered to adopt certain Common Specifications in lieu of harmonised standards. As yet, no such Common Specifications have been adopted.

CONFORMITY ASSESSMENT PROCEDURES

As well as allowing Internal Production Control, EU-Type Examination followed by Conformity to Type, and Full Quality Assurance, the CRA introduces a new conformity assessment procedure, the European Cybersecurity Certification Scheme ("EUCC"). As yet, no such EUCC has been adopted, although the EC has the power under Article 8(1) of the CRA to adopt such schemes.

Article 32 of the CRA, much like Article 17 of the RED, specifies that manufacturers may only use certain conformity assessment procedures depending on certain factors. In the case of the CRA, this is based not only on the application of Harmonised Standards as cited in the OJEU but also on these established Common Specifications, and further divided based on the equipment category.

- For product types not listed as important (in Annex III) or critical (in Annex IV), any of the four conformity assessment procedures are allowed.
- For product types listed as Class I important (in Annex III):
    - If the manufacturer has fully applied Harmonised Standards or Common Specifications, they may use any of the four CAPs above.
    - If the manufacturer has not fully applied Harmonised Standards or Common Specifications, they must follow EU-Type Examination followed by Conformity to Type, Full Quality Assurance, or an EUCC Scheme at assurance level 'substantial' or higher.
- For product types listed as Class II important (in Annex III), the manufacturer must follow EU-Type Examination followed by Conformity to Type, Full Quality Assurance, or an EUCC Scheme at assurance level 'substantial' or higher.
- For product types listed as critical (in Annex IV), the manufacturer must follow an EUCC Scheme, or, where a relevant EUCC scheme does not exist for the product type, they may use EU-Type Examination followed by Conformity to Type or Full Quality Assurance.

UNDERSTANDING THE CYBER SECURITY LEGISLATION

REPORTING OBLIGATIONS

As well as the product compliance requirements which take effect in 2027, the CRA includes reporting obligations for manufacturers which become mandatory from September 11th, 2026. To coordinate this, each member state is required to designate a single computer security incident response team ("CSIRT") as their coordinator of such reporting.

To comply with the reporting obligations, manufacturers who become aware of any actively exploited vulnerability in their product or a severe incident having an impact on the security of the product must:

- Notify the European Union Agency for Cybersecurity ("ENISA").
- Notify the CSIRT in the relevant member state (see Article 7 of the CRA for details on how to determine which member state's CSIRT to notify).
- Notify users of the affected product, including with details on any corrective actions the user could take to mitigate the impact.

An incident shall be considered to be a severe incident having an impact on the security of the product where it negatively affects or is capable of negatively affecting the ability of a product to protect the availability, authenticity, integrity, or confidentiality of sensitive or important data or functions; or it has led or is capable of leading to the introduction or execution of malicious code in a product or in the network and information systems of a user of the product with digital elements.

The notifications to ENISA and the CSIRT must be submitted via the single reporting platform established by ENISA, however, at the point of writing this document, such a platform does not yet exist.

RISK ASSESSMENT

There is a requirement under the CRA for a manufacturer to undertake an assessment of the cybersecurity risks associated with their product, and to take the outcome of that assessment into account during the planning, design, development, production, delivery, and maintenance phases of the product with a view to minimising cybersecurity risks, preventing incidents, and minimising their impact. This is similar to the risk assessment required under the RED.

PLACING ON THE MARKET

As with all CE marking directives and regulations, these new CRA requirements apply at the point a product is placed on the market. That should be read as meaning each individual unit, not a product type or a production run. Products which are placed on the market from December 11th, 2027 must meet the applicable requirements at that point in time, regardless of whether that same product type was available before that date or not.

DECLARATION OF CONFORMITY AND CE MARKING

There are no additional product marking requirements, however the declaration of conformity (DoC) should be updated to reference the CRA and any standards used in assessing the products against these requirements. If an EU-Type Examination Certificate has been issued by a Notified Body, this should be listed on the DoC. The new DoC will need to be signed and dated at that point.

UNDERSTANDING THE CYBER SECURITY LEGISLATION

OTHER STANDARDS

EN 303 645 and EN 18031 are not the only standards aiming to address product cyber security. Other standards such as IEC 62443-2-4, IEC 15408, and ISO 21434 all address similar areas. Fundamentally, each of these standards is aiming to give a methodology to answer the question "is this product cyber secure?" While they may approach this from different angles, a product which is cyber secure should in theory pass an assessment to any of the standards. This is no different to the situation with, for example, automotive EMC standards and industrial EMC standards – these standards all aim to address the same question of whether the device is electromagnetically compatible, but because they have been written by different groups, at different points in time, and with different product types in mind, they approach the question in very different ways.

A mapping document, TS 103 929, has been published by ETSI and can be used to show the mappings between EN 303 645, the RED requirements, and IEC 62443-4-2.

WHAT DOES A CYBER ASSESSMENT LOOK LIKE?

A product cyber security assessment will largely be documentation-based, with a relatively small amount of product testing. Typically, the first phase will be a review of the documentation submitted by the manufacturer to a test lab, followed by a functional assessment and a completeness assessment, which will involve product testing.

The product testing can be described as grey-box testing, an interim between white-box testing (in which the tester has intricate knowledge of the product workings) and black-box testing (in which the tester has zero knowledge of the product workings). The manufacturer will be required to provide support to the tester to allow them access to certain device functions, update mechanisms, or cryptographies, etc. Without this level of support the tester will be unable to complete much of the assessment.

DOCUMENTATION

The different standards above will refer to the required documentation by different terms, but generally will fall under one of three categories:

- An Implementation Conformance Statement ("ICS") lists the mechanisms, provisions, or protections that a device implements in order to be cyber secure. The ICS will often also act as a signposting document between specific documentation requests within the standard (e.g. "provide a list of all network assets processed by the product") and the manufacturer's documentation (e.g. "see section 4 of the user guide" or "see at Evidence1.docx"). TS 103 645 specifically requests an ICS from the manufacturer. The EN 18031 standards do not.
- An Implementation Extra Information for Testing ("IXIT") contains additional necessary information to perform the assessment. Typically, one IXIT is provided for each mechanism, provision, or protection that a device implements. TS 103 645 specifically requests IXITs from the manufacturer. The EN 18031 standards do not refer to an IXIT specifically, but request multiple items of supporting documentation (referred to as "E.Info" and "E.Just" documents in the standards) which are in effect IXITs.
- Decision Trees can be used to assess whether a product meets a particular clause of a given standard by answering a series of structured yes/no questions, and ending in a pass, fail, or N/A outcome. These decision trees are unique to the EN 18031 standards, which specifically request that they are provided by the manufacturer.

The test lab will typically review the documentation and provide feedback or corrective actions to the manufacturer, and this back-and-forth process may go through multiple iterations before both parties are satisfied that the provided documentation adequately address all points in the relevant standard(s).

FUNCTIONAL SUFFICIENCY ASSESSMENT

The purpose of a functional sufficiency assessment is to verify that each mechanism, provision, or protection that is claimed in the documentation provided by the manufacturer is present on the equipment and operates as intended. Some examples of this would include the following:

- In the case where a physical external interface is provided, and the manufacturer claims that the data transmitted over this interface is encrypted, the test lab would typically verify that the data transmitted over this interface is encrypted and is not, for example, sent as plaintext.
- In the case where a PIN pad is provided, and the manufacturer's documentation claims that the PIN pad will lock for a period after a number of incorrect PIN entries, the test lab would typically verify that this does occur.
- In the case where a data input exists, and the manufacturer's documentation claims that any inputted data is validated for structure or length etc., the test lab would typically verify that correctly-formed data provided to the input is processed and that malformed data provided to the input is properly rejected.

The test lab would not be expected to attempt to overcome any of these protections, just to verify that they are present and operational.

UNDERSTANDING THE CYBER SECURITY LEGISLATION

COMPLETENESS ASSESSMENT

The completeness assessment aims to verify that the documentation that has been provided covers all aspects of the product. The test lab would likely check through visual inspection or through the use of network scanning tools that no physical or over-the-air interfaces exist on the product that are not described in the ICS and/or IXITs, and would likely check the user documentation to ensure that no product features exist which are not properly described in the ICS and/or IXITs.

ROLE OF TEST LABS

There is no obligation under any of the standards or legislation above to use a third-party testing laboratory. This is similar to the situation for other test disciplines, like EMC. Most manufacturers, however, will not have the capability to perform all EMC tests internally, and therefore approach a test lab for this – the same will be true of cyber security assessment. Equally, those manufacturers who do have capabilities internally for EMC testing often value the assessment of an independent third-party.

PENETRATION TESTING

Penetration testing refers to a method for assessing the security of a product by attempting to breach some or all of that product's security measures using the same tools and techniques as an adversary might. Exactly what techniques are used and how much knowledge of the system is given to the testers beforehand can vary between test regimes.

None of the standards detailed above, or any of the legislation discussed, require penetration tests to be carried out.

HOW CAN ELEMENT HELP?

Element supports equipment manufacturers with end-to-end Advisory, Testing, Inspection, and Certification (ATIC) and Global Market Access (GMA) solutions, worldwide. Our local teams of global experts support customers to meet the ever-changing compliance requirements, making the compliance process straightforward.

For support with these new cyber security requirements, we can help you in three main ways:

1. Our Advisory Services department can create a compliance strategy document or test plan for your product, outlining the path to market and reducing uncertainty. We can support with risk assessment, technical file compilations, and can review Declarations of Conformity or Statements of Compliance to ensure the requirements have been met in full.
2. We are an ISO 17025 accredited test lab, and our Smart Technologies test engineers are well-equipped to support with cyber security testing for a range of product types.
3. We are an ISO 17065 accredited Certification Body, and a Notified Body under the Radio Equipment Directive. We can issue EU-Type Examination Certificates against the RED, either when required as Harmonised Standards have not been fully applied, or as an optional service to confirm compliance.

To learn more about how our global teams of specialists can help your business, contact us today to discuss your testing and compliance requirements.

RELATED SERVICES

- Advisory services
- Pre-compliance
- Safety testing
- SAR testing
- Radio testing
- EMC testing
- Protocol testing (Matter & Zigbee)
- Cyber Security
- Global Market Access (GMA)

> "By August 1st 2025, any products sold in the EU must be compliant with the cyber security changes in the Radio Equipment Directive"

Michael Derby
Technical Director

ABOUT ELEMENT

Element is a leading global provider of Testing, Inspection, and Certification (TIC) services on a wide range of products, materials, processes and services and products for a diverse set of end markets, where failure in service is simply not an option.

270+

Laboratories located in 30 countries within the Americas, Europe, Middle East, Africa, Asia, and Australia

9000+

Employees and Engaged Experts worldwide, ready to help you meet your testing requirements

1000+

Accreditations and approvals. An independent endorsement of the quality of service we deliver

55000+

Customers served worldwide in a diverse range of market-leading scientific, technical, and engineering industries

element

contactus@element.com | Americas +1 833 373 1504 | Europe & Rest of World +44 800 470 3487 | Asia +82-31-339-9970

ELEMENT.COM/WIRELESS-RADIO-TESTING