Fact Sheet v2

Electronic fire safety and security products in the context of important and critical products defined by the Cyber Resilience Act (CRA)

Introduction

The Cyber Resilience Act (CRA, (EU) 2024-2847) has been published in Official Journal of the EU (OJEU) in November 2024 setting horizontal cybersecurity requirements for products that process and communicate digital data, including their remote data processing solution if any. This Regulation shall apply as from 11 December 2027 (provisions related to the reporting obligations of the manufacturers (Article 14) shall apply as from 11 September 2026 and provisions related to the notification of the conformity assessment bodies shall apply as from 11 June 2026).

The essential requirements on the products in scope of the CRA and on the process for vulnerability handling put in place by the manufacturer are introduced in Article 6 and detailed in Annex I of the CRA. Those essential requirements are the same for all the products in scope of the CRA.

Specific categories of Important and Critical products are defined in Articles 7 and 8 and listed in Annex III and Annex IV of the CRA. Furthermore, the technical description of those categories has been laid down in the Implementing Regulation (EU) 2025/2392 published in the OJEU in December 2025. The purpose of defining those categories is to impose for those products a conformity assessment procedure that is stricter than the one for the "default" products (products that are neither categorised as Important nor as Critical).

Understanding those categories of products is therefore of paramount importance to comply with the provisions of the CRA. The purpose of this fact sheet is to explain how the conformity assessment procedures are assigned to the categories of products and which electronic fire safety and security products fit into those categories.

Some types of products are explicitly commented. Those should be considered as illustrating examples. The present fact sheet does not pretend being exhaustive and other fire safety or security products that are not addressed (e.g. video cameras) might also belong to a particular category and be added to this document in a future release.

Conformity assessment procedures

The conformity assessment procedure to be applied for a product is defined in Article 32 of the CRA.

- For the "default" products, self-assessment and self-declaration of conformity (Module A) are allowed regardless of whether the technical standard used to test the products is cited in the OJEU or not. However, products complying with the requirements of a harmonised standard cited in the OJEU do benefit of presumption of conformity (Article 27), others do not. For electronic fire safety products and physical security products belonging to that "default" category, compliance can be demonstrated by using, for example, the broad vertical standards EN 62443-4-x (extending the IEC 62443 series to cover all the essential requirements of the CRA) under development in CLC/TC 65X or the horizontal standards (EN 40000-x) under development in CEN/CLC/JTC 13.
- For the products categorised as Important Class I, self-assessment and declaration of conformity (Module A) is allowed only where the technical standard used to test the products is cited in the OJEU. Where such a standard does not exist for that product or where the manufacturer has not

Copyright Euralarm © 2026, Zug, Switzerland

fully applied such a standard, the product shall be tested by a notified body (EU-type examination, Module B) and the manufacturer shall apply an internal production control (Module C).

- For the products categorised as Important Class II, self-assessment and self-declaration of conformity are not allowed. The product shall be tested by a notified body (EU-type examination, Module B) and the manufacturer shall apply an internal production control (Module C).
- For the products categorised as Critical, the conformity assessment procedure depends on the availability of a delegated act covering the category of product. The European Commission may adopt delegated acts assigning a European cybersecurity certification scheme (developed by ENISA under the Cyber Security Act, e.g. EUCC on Common Criteria) to a certain category of Critical products. Where such a delegated act exists, the manufacturer shall apply the assigned certification scheme. No such delegated act is existing today. By default, the product shall be tested by a notified body (EU-type examination, Module B) and the manufacturer shall apply an internal production control (Module C).

Important and critical product categories

Introduction

Annex III of the CRA lists 19 categories of Important Class I products and 4 categories of Important Class II products:

<table>
<tr><th colspan="2">Class I</th></tr>
<tr><td>1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers
2. Standalone and embedded browsers
3. Password managers
4. Software that searches for, removes, or quarantines malicious software
5. Products with digital elements with the function of virtual private network (VPN)
6. Network management systems
7. Security information and event management (SIEM) systems
8. Boot managers
9. Public key infrastructure and digital certificate issuance software
10. Physical and virtual network interfaces
11. Operating systems
12. Routers, modems intended for the connection to the internet, and switches
13. Microprocessors with security-related functionalities</td><td>14. Microcontrollers with security-related functionalities
15. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities
16. Smart home general purpose virtual assistants
17. Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems
18. Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council (1) that have social interactive features (e.g. speaking or filming) or that have location tracking features
19. Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or (EU) No 2017/746 do not apply, or personal wearable products that are intended for the use by and for children</td></tr>
<tr><th colspan="2">Class II</th></tr>
<tr><td>1. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments
2. Firewalls, intrusion detection and prevention systems</td><td>3. Tamper-resistant microprocessors
4. Tamper-resistant microcontrollers</td></tr>
</table>

Annex IV lists 3 categories of Critical products:

1. **Hardware Devices with Security Boxes**
2. Smart meter gateways within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 of the European Parliament and of the Council (1) and other devices for advanced security purposes, including for secure cryptoprocessing
3. Smartcards or similar devices, including secure elements

According to Articles 7 and 8 of the CRA and as explained in the FAQ document published by the European Commission, a product belongs to one or more categories of Important or Critical products where **its core functionality** is the one described in the technical description of the Implementing Regulation (EU) 2025/2392. It is important to note that a product embedding a functionality described as Important or Critical doesn't make that product Important or Critical where its core functionality is not categorised as such. For example, a microcontroller with security-related functionalities placed as such on the EU market shall be categorised as Important product Class I. However, the core functionality of a Control and Indicating Equipment (CIE) for fire detection in a commercial or industrial environment incorporating such a microcontroller is to process inputs from fire detectors and to trigger a fire alarm, which is not listed as an Important or Critical core functionality. That CIE therefore belongs to the "default" category.

Three categories have some touch points with products in the electronic fire safety and security sector. They are highlighted in bold characters in the tables above and are commented in the following sections.

Smart home products with security functionalities

This category #17 of Important Class I products is described in the Implementing Regulation as follows:

> *Products with digital elements that protect the physical security of consumers in a residential setting and which can be controlled or managed remotely from other systems, as well as hardware and software that centrally control such products.*
>
> *This category includes but is not limited to smart door locking devices, baby monitoring systems, alarm systems and home security cameras.*

4 criteria need to be met for a product to belong to that category:

- "protect the physical security": the core functionality of the product is the protection of the physical security, e.g. protection against attack, intrusion, fire, poisonous gases or flammable gases;
- "of consumers": the intended use of the product includes the protection of consumers;
- "in a residential setting": the intended operating environment of the product includes a residential environment, regardless of whether it is also intended for commercial or industrial environments;
- "can be controlled or managed remotely from other systems": the product itself is intended to be controlled or managed from a system that can be located in a remote location, typically via the cloud (control or management from a CIE in the same supervised premises is not considered here).

The Table below lists some examples and justifies why those products do or don't belong to that category.

Example description	In scope of CRA	Belongs to category Important Class I #17
Control panel for intrusion detection in a residential environment	**YES,** it incorporates digital data connection with another device or network	The core functionality is to protect the physical security of consumers in a residential environment (regardless of whether it is also intended for commercial or industrial environments)
— with features for remote access		**YES,** it can be controlled or managed through a remote access infrastructure
— with transceiver for alarm transmission via IP protocol and without features for remote access		**NO** (belongs to default category), it cannot be controlled or managed through a remote access infrastructure and alarm transmission on itself is not a means for control or management of the product
Keypad for user interaction with a control panel for intrusion detection in a residential environment	**YES,** it incorporates digital data connection with another device or network	The core functionality is to protect the physical security of consumers in a residential environment (regardless of whether it is also intended for commercial or industrial environments)
— sending and receiving digital messages through a local connection to and from the control panel only		**NO** (belongs to default category), it cannot be controlled or managed through a remote access infrastructure
— with features for receiving control or management commands from the internet		**YES,** it can be controlled or managed through a remote access infrastructure
Intrusion detector for use in a residential environment		The core functionality is to protect the physical security of consumers in a residential environment (regardless of whether it is also intended for commercial or industrial environments)
— signalling states to the CIE via OPEN/CLOSE signals only	**NO,** it doesn't incorporate a digital data connection with another device or network	**NO,** this product is not in scope of the CRA
— sending and receiving digital messages through a local connection to or from the CIE only	**YES,** it incorporates digital data connection with another device or network	**NO** (belongs to default category), it cannot be controlled or managed through a remote access infrastructure (the CIE might be remotely controlled but the detector is controlled by the CIE)
— with features for receiving control or management commands from the internet	**YES,** it incorporates digital data connection with another device or network	**YES,** it can be controlled or managed through a remote access infrastructure
CIE for fire detection in a commercial or industrial environment with features for remote access	**YES,** it incorporates digital data connection with another device or network	**NO** (belongs to default category), the core functionality is to protect the physical security of consumers in a non-residential environment

Example description	In scope of CRA	Belongs to category Important Class I #17
Smoke alarm device or CO alarm device		The core functionality is to protect the physical security of consumers in a residential environment
— without interconnection	**NO,** it doesn't incorporate a digital data connection with another device or network	**NO,** this product is not in scope of the CRA
— with local interconnection to another alarm device or to a local control panel	**YES,** if it incorporates digital data connection with another device or network	**NO** (belongs to default category), it cannot be controlled or managed through a remote access infrastructure
— with features for receiving control or management commands from the internet	**YES,** it incorporates digital data connection with another device or network	**YES,** it can be controlled or managed through a remote access infrastructure
Software placed on the EU market that is intended to be implemented in the cloud and that manages the remote access to an alarm system in residential environment	**YES,** it incorporates digital data connection with another device or network	**YES,** its core functionality is to protect the physical security of consumers in a residential environment and it centrally controls CIEs
Software placed on the EU market that is intended to be implemented in the cloud and that manages the transmission of alarms generated in a residential environment	**YES,** it incorporates digital data connection with another device or network	**YES,** its core functionality is to protect the physical security of consumers in a residential environment and it centrally controls the transmission of alarms

This category of products is intended to be covered by the future harmonised standard EN 304 632 currently drafted by ETSI TC CYBER.

Identity management systems and privileged access management

This category #1 of Important Class I products is described in the Implementing Regulation as follows:

> *Identity management systems are products with digital elements that provide mechanisms for authentication or authorisation and that may also provide mechanisms for the lifecycle management of identity credentials of natural persons, legal persons, devices or systems, such as identity registration, provisioning, maintenance, deregistration. These systems include access management systems that control access of natural persons, legal persons, devices or systems to digital resources or physical locations.*
>
> *Privileged access management software is an access management system that controls and monitors access rights to IT or OT systems and sensitive information within an organisation, including systems enforcing differentiated access control policies for privileged users.*
>
> *This category includes but is not limited to authentication and access control readers, biometric readers, single sign-on software, federated identity management software, one-time password software, hardware authentication devices such as transaction authentication number (TAN) generators, authentication software and multi-factor authentication software.*

This category targets access control devices and systems to digital resources (logical access) and to physical locations (physical access). Regarding physical access, the following elements need to be considered:

- Physical access control solution is seen as an Operational Technology (OT) system and is controlled by access management software. The system is intended to enforce access control policies for privileged users who can access physical locations of the building.
- The operation of the physical access control solution (OT) is linked to access control readers in all formats and Mobile apps (mobile credentials).
- Physical access control system is also linked to identity management and Software to manage those identities: a database of users (credentials) linked to an identity (user) who may or may not have access rights.

The Table below lists some examples and justifies why those products do or don't belong to that category.

Example description	In scope of CRA	Belongs to category Important Class I #1
CIE of an electronic access control system for controlling the physical access of persons to a building or an area	**YES,** it incorporates digital data connection with another device or network	**YES,** its core functionality is to manage access based on identity privileges, it stores identities linked to credentials and access rights
Access control software running on a remote server	**YES,** it incorporates digital data connection with another device or network	**YES,** its core functionality is to manage access based on identity privileges, it stores identities linked to credentials and access rights
Access control reader (e.g. biometric reader, tag reader) of an electronic access control system for controlling the physical access of persons to a building or an area	**YES,** it incorporates digital data connection with another device or network	
— not managing itself the identity of the users		**NO** (belongs to either default category or to cat. #17): — this tag reader is not managing itself the identities of the users (the identities are not stored on the reader) — even though the tag reader may incorporate a software managing privileged access, it is a hardware product
— managing itself the identity of the users		**YES,** its core functionality is identity management (the identities are stored on the reader)
Access control credential (e.g. physical tag)	**YES,** it incorporates digital data connection with another device or network	**NO** (belongs to either default category or to cat. #17): its core function is to contain credential data but it is static and does not to manage identities
CIE for fire detection or intrusion detection	**YES,** it incorporates digital data connection with another device or network	**NO** (belongs to either default category or to cat. #17), even though the CIE incorporates a software managing privileged access to its resources (access level management), its core functionality is neither identity management nor privileged access management

Example description	In scope of CRA	Belongs to category Important Class I #1
Biometric reader of an intrusion detection system and placed on the EU market separately from the CIE	**YES,** it incorporates digital data connection with another device or network	
— not managing itself the identity of the users		**NO** (belongs to either default category or to cat. #17): — this biometric reader is not managing itself the identities of the users (the identities are not stored on the reader) — even though the biometric reader may incorporate a software managing privileged access, it is a hardware product
— managing itself the identity of the users		**YES,** its core functionality is identity management (the identities are stored on the reader)
Tag reader for unsetting an intrusion alarm system and placed on the EU market separately from the CIE	**YES,** it incorporates digital data connection with another device or network	
— not managing itself the identity of the users		**NO** (belongs to either default category or to cat. #17): — this tag reader is not managing itself the identities of the users (the identities are not stored on the reader) — even though the tag reader may incorporate a software managing privileged access, it is a hardware product
— managing itself the identity of the users		**YES,** its core functionality is identity management (the identities are stored on the reader)
Software placed on the EU market that is intended to be implemented in the cloud and that manages the remote access to an access control system	**YES,** it incorporates digital data connection with another device or network	**YES,** its core functionality is to manage access based on identity privileges, it stores identities linked to credentials and access rights

This category of products is intended to be covered by a future harmonised standard currently drafted by CEN/TC 224.

Hardware Devices with Security Boxes

This category #1 of Critical products is described in the Implementing Regulation as follows:

> *Hardware products with digital elements that securely store, process, or manage sensitive data or perform cryptographic operations, and that consist of multiple discrete components, incorporating a hardware physical envelope providing tamper evidence, resistance or response as countermeasures against physical attacks.*
>
> *This category includes but is not limited to physical payment terminals, hardware security modules that generate and manage cryptographic elements, and tachographs that meet the above description.*

Intrusion detection products and electronic access control products perform cryptographic operations (e.g. to comply with CRA essential requirements) and provide tamper resistance and response. However, those functions

do not constitute the core functionality of those products. Therefore, they don't belong to that category of Critical products.

This category of products is intended to be covered by a future harmonised standard currently drafted by CEN/TC 224.

Conclusion

The essential requirements laid down in the CRA are the same for all the products in scope, regardless of their categorisation.

The CRA defines categories of Important and Critical products. Those categories determine the conformity assessment procedure to be followed by the manufacturer before placing products on the EU market. It is the responsibility of the manufacturer to adequately categorise the products and to apply the corresponding provisions of the Regulation.

Based on the available facts (CRA, Implementing Regulation and FAQ), a limited sub-set of electronic safety products and some intrusion detection products belong to the category of Important product Class I "smart home products with security functionalities" and some electronic access control products belong to the category of Important product Class I "identity management systems and privileged access management". For those products, the full application of the corresponding harmonised standard cited in the OJEU will be needed to benefit from self-assessment procedure and presumption of conformity. No fire safety or physical security products have been identified under the category of Critical products "hardware devices with security boxes". Hence, most of the electronic fire safety and physical security products belong to the "default" category and the conformity with the essential requirements of the CRA can be demonstrated by using any standard that the manufacturer can prove it covers all the CRA essential requirements, e.g. EN 62443-4-x under development in CLC/TC 65X or the horizontal standards under development in CEN/CLC/JTC 13.

Zug, 5 November 2026

About Euralarm

Euralarm represents the fire safety and security industry, providing leadership and expertise for industry, market, policy makers and standards bodies. Our members make society safer and secure through systems and services for fire detection and extinguishing, intrusion detection, access control, video monitoring, alarm transmission and alarm receiving centres. Founded in 1970, Euralarm represents over 5000 companies within the fire safety and security industry valued at 67 billion Euros. Euralarm members are national associations and individual companies from across Europe.

Gubelstrasse 11 • CH-6300 Zug • Switzerland

E: secretariat@euralarm.org
W: www.euralarm.org

DISCLAIMER

This document is intended solely for guidance of Euralarm members, and, where applicable, their members, on the state of affairs concerning its subject. Whilst every effort has been made to ensure its accuracy, readers should not rely upon its completeness or correctness, nor rely on it as legal interpretation. Euralarm will not be liable for the provision of any incorrect or incomplete information.

Note: The English version of this document is the approved Euralarm reference document.