

Engineering CRA-Ready Products by Design

September 2026

brightsight By SGS

Infineon

Public



EU CRA essentials

01

Navigating the EU CRA with Infineon

Introduction to the EU CRA compliance

02

Get ready for EU Cyber Resilience Act with Infineon

EU CRA for Consumers and Industrial Sectors

03

Understanding EN 50764: The CRA Harmonized Standard for Smartcard and Secure Element Platforms

EU CRA Cybersecurity Requirements

Copyright © Infineon Technologies AG 2026. All rights reserved.

Speakers of today‘s webinar



Preeti Ohri Khemani

Infineon Technologies,
Senior Director Partnership and Ecosystem Management



Erik Wood

Infineon Techologies,
Senior Director of Microcontroller Cryptography and Product Security



Xavi Castells

Brightsight,
Director of Strategic Developments

Copyright © Infineon Technologies AG 2026. All rights reserved.

EU CRA – why is it relevant for you





Copyright © Infineon Technologies AG 2026. All rights reserved.




brightsight
By SGS

Today‘s Agenda

CRA Policy (recap) and Standards Update
“where are we today?”

01

Risk Analysis & Threat Modeling
“where do you begin?”

02

Engineering the Compliance
“what are the next steps?”

03



Copyright © Infineon Technologies AG 2026. All rights reserved.



Segment 1: CRA Policy (recap) and Standards Update

Preeti Ohri Khemani

Public

CRA is raising security baselines for digital connected products

What is the EU CRA?

The EU Cyber Resilience Act (CRA) sets essential cybersecurity standards for IoT, smart home devices, Industrial Automation and Control Systems, and all digital connected products to be sold in the EU single market from December 2027 onwards.

It mandates security by design and by default, enabling products to be secured throughout their lifecycle.

Where does it apply to?

The CRA applies to most hardware and software with digital elements, except for:

- Non-commercial projects and open-source software*
- Cloud services without physical components
- Devices in automotive, healthcare, and aviation that are already covered by specific EU regulations.

Note: * When open source SW is integrarted into a commerial products then manufacturers are obligated to comply with CRA for that part.

Copyright © Infineon Technologies AG 2026. All rights reserved.

EU CRA Essential Requirements for getting the CE label



Product Security Outcomes

Product security outcomes should be included based on product's **cybersecurity risk** in its operational environment.



Vulnerability Management Process

Strict incidence reporting timelines of 1-3-14 days and vulnerability handling - **security updates** (min. 5 years).



Information & Labelling

Publish support information (duration, type, contact), product's primary function and relevant security instructions.

Copyright © Infineon Technologies AG 2026. All rights reserved.

CRA Product Categories and their Compliance Requirements

'catch-all category'	Examples	Examples	Examples
All products with digital elements (HW, SW, including remote data processing) **not listed** in important, critical, or exempted product categories	Industrial and smart home devices with security functions, routers, modems, connected toys, wearables, biometric, access control,…	Hypervisors and container runtime environments, VPN, Firewalls, Tamper-resistant Microcontrollers, and Microprocessors, …	Smart meter gateways, advanced security systems, smartcards, secure elements and similar devices, …
Default "Class 0"	**Important products "Class I"**	**Important products "Class II"**	**Critical products**

Self asssessment

Self Assessment based on EU harmonized standard*

3rd Party Assessment: Internal Production Control, Full QA

EU cybersecurity certification**

* EU harmonized standards development are commissioned by EU Commission; in absence, 3rd Party assessment by Notified bodies is required
** Direct use of EU cybersecurity certification as a CRA demonstration conformity can be allowed through a EU Delegated Act.

Copyright © Infineon Technologies AG 2026. All rights reserved.

CRA Regulatory and Standardization timelines



December 10, 2024

Publication of the EU Cyber Resilience Act final text

September 11, 2026

Mandatory incidence reporting obligations started to apply (Article 14)

CRA SRP landing page

December 31, 2026
(prev. Oct. 30, 2026)

Delivery deadline for Type C product-specific vertical standards

December 11, 2027

Full compliance required for digital connected products sold in the EU single market

June 11, 2026

Notification of Conformity Assessment Bodies rules started to apply (Chapter IV, Articles 35-51)

NANDO Database

October 31, 2026
(prev. Aug. 30, 2026)

Delivery deadline for Type A framework standards and Type B vulnerability handling standards

October 30, 2027

Delivery deadline for remaining Type B technical controls standards

Copyright © Infineon Technologies AG 2026. All rights reserved.

CRA Harmonized Standards development in three groups

CENELEC EUROPEAN COMMITTEE FOR ELECTROTECHNICAL STANDARDIZATION

CEN EUROPEAN COMMITTEE FOR STANDARDIZATION

ETSI

Type A
Horizontal (Framework)

Focus: Core principles, risk methodologies, vocabulary.

- EN 40000-1-1: Vocabulary and Terminology
- EN 40000-1-2: Principles for Cyber Resilience includes risk assessment framework, secured-by-design process, and cybersecurity lifecycle activities

Type B
Horizontal (Operational)

Focus: Vulnerability lifecycles, SBOMs, generic patch delivery.

- EN 40000-1-3: Vulnerability handling requirements, Software Bill of Materials (SBOMs), triage and patching
- EN 40000-1-4: Generic product security requirements catalog mapping essential requirements to generic security controls
- EN 40000-1-5: Threat analysis and security Documentation Requirements

Type C
Vertical (Specific)

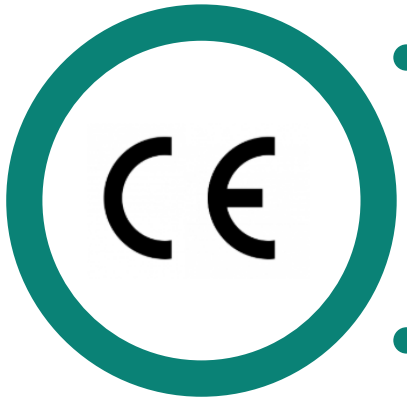
Focus: Technical criteria for families of devices and software products.

- prEN 5076x: Security semiconductors in CRA Important, Critical categories
- prEN 18330, prEN 40000-10: Identity management; privileged access systems
- EN 50770 / IEC 62443 Profiles for Operational Technology devices
- ETSI EN 304 6xx series for IT & Consumer Products

Note: All are still draft stage → Knowing which group of standards is applicable to your products tells you what to read.

Copyright © Infineon Technologies AG 2026. All rights reserved.

Begin your CRA engineering journey right now



- Design against CRA Annex I directly
- Get vulnerability handling orgaization and process working
- Keep the evidence as you go
- Decide and publish the support period
- Check your devices’ product class, read/apply the draft standards

Copyright © Infineon Technologies AG 2026. All rights reserved.



Building digital trust

CRA Webinar

Segment 2:
Risk analysis & Threat modeling

17/09/2026

Xavi Castells

Classification Policy: UNCLASSIFIED

brightsight

By SGS



Overview

The purpose of this webinar is to understand:

- Why the CRA requires a risk assessment
- What manufacturers are expected to demonstrate
- A practical approach to CRA risk assessment
- How supplier evidence can be reused
- Why product composition remains the OEM's responsibility

brightsight

By SGS

Why Are We Talking About Risk Assessment?

Risk Assessment is a Core CRA Requirement

- The CRA requires manufacturers to identify, assess, mitigate and monitor cybersecurity risks throughout the product lifecycle. [Article 13(2)-(7)]

Regulatory Framework

- **Annex I Part I:** Defines the legal obligation.
- **EN 40000-1-2:** Main risk management standard.
- **EN 40000-1-3:** Vulnerability handling.
- **EN 40000-1-4:** Security requirements and controls

Guidance

- **ENISA Secure by Design and Default Playbook**
- **BSI Technical Guideline TR-03183-1**

What Does CRA Actually Expect?

What does the CRA expects

- Defined the product context and intended use
- Defined risk acceptance criteria and methodology
- Identified assets and security objectives
- Identified threats and vulnerabilities
- Assessed and prioritized risks
- Implemented appropriate security measures
- Managed residual risk
- Maintained the assessment throughout the product lifecycle

CRA does not mandate a specific methodology

The CRA does not require manufacturers to use a particular approach such as:

- STRIDE, Attack Trees, OCTAVE, EVITA, CVSS, ISO/IEC 27005

Established risk management frameworks can be leveraged as a starting point.

CRA is outcome-focused: the methodology is flexible, but the process must be systematic, documented and justified.

brightsight
By SGS

Practical CRA Risk Assessment

A 5-step approach



Product context

What are we building?



Identify assets

What are we protecting?



Identify threats and vulnerabilities

What could go wrong?



Assess the risk

What matters most?



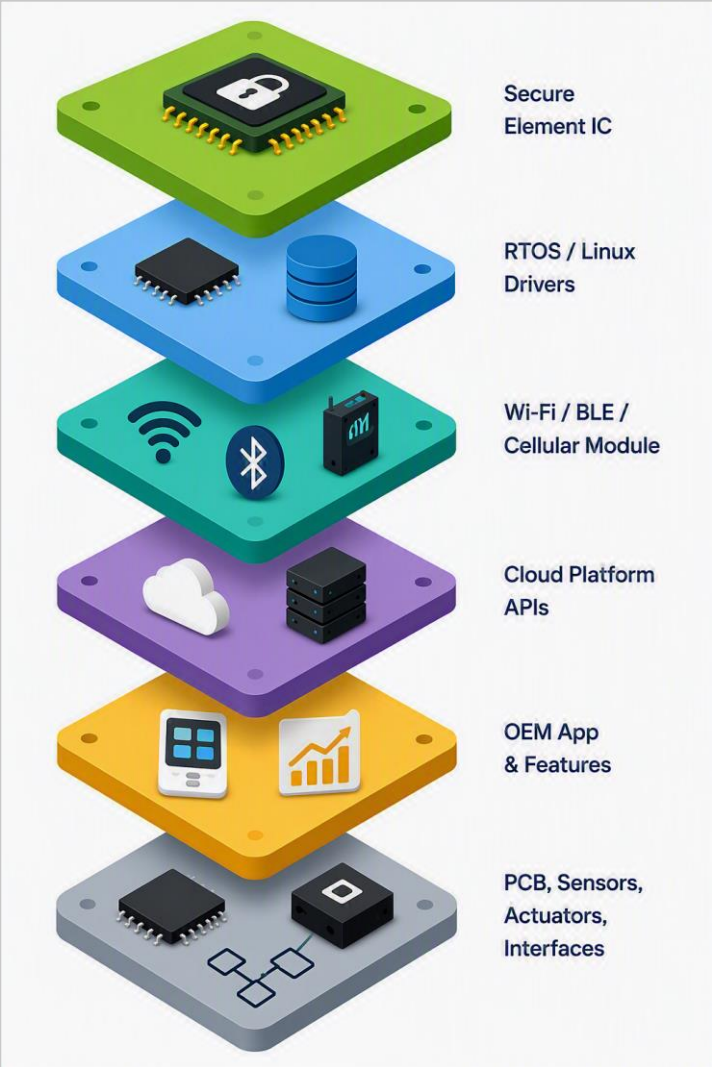
Define security measures

How do we reduce the risk?

brightsight

By SGS

The Challenge of Composition



Good news

Component suppliers may already provide:

- Security certifications
- Threat analysis
- Risk assessments
- Security objectives
- Security architectures
- Vulnerability management evidence

These artefacts can significantly reduce the effort required by the OEM.

The challenge: new risks

Even when individual components have been independently assessed, the final product introduces:

- New interfaces
- New trust relationships
- New configurations
- New data flows
- New attack paths

These risks only emerge when components are combined.

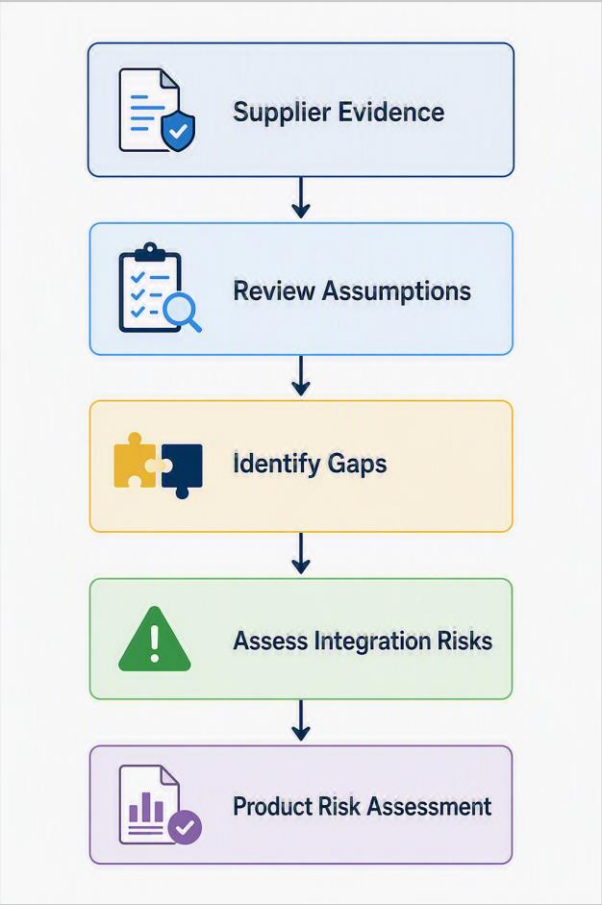
The final product risk assessment cannot be obtained by simply combining component risk assessments.

brightsight

By SGS

Reusing Supplier Evidence

Reuse strategy



What can be reused?

Supplier Evidence	How it supports CRA
Threat Analysis	Threats and assumptions
Risk Assessment	Risks and mitigations
Security Architecture	Product understanding
Certifications & Test Reports	Validation evidence and/or independent assurance evidence
Vulnerability Handling Process	Operational security evidence
Software Bill-of-Materials	Component inventory and vulnerability monitoring
Vulnerability Information	Known vulnerabilities and remediation history

brightsight
By SGS

Key Takeaways

- OEMs remain responsible for the risk assessment of the final product, including supplier components.
- CRA requires a documented risk-based approach.
- CRA defines the objective, not the methodology
- Leverage existing standards, frameworks and industry practices.
- Reuse supplier evidence whenever possible.
- Focus on risks introduced by the final product and its integration
- Keep it simple and continuously improve over the product lifecycle.

Don't reassess every component. Reuse trusted supplier evidence, use a methodology that fits your organization, and focus on understanding the risks introduced by the final product.



Thank you!
Questions?

Contact us:
brs.sales@sgs.com
+31 (0) 15 269 2500
www.brightsight.com

© SGS Société Générale de Surveillance SA (2026)

brightsight
By SGS



Segment 3: Engineering the Compliance using Infineon Microcontrollers

Erik Wood

Public

PSOC™ Secured MCUs

PSOC™ EDGE



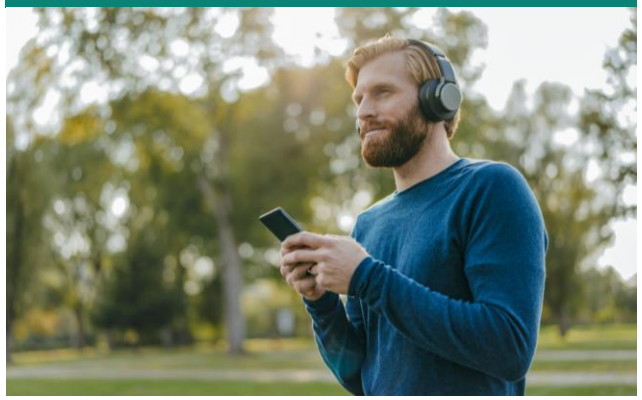
Best-in-class MCU for Edge AI applications allowing customers to create differentiated products for the IoT era while protecting their IPs (models). Staged AI pipeline enables unrivaled performance to power ratio.

PSOC™ CONTROL



Industrial MCU family maximizing software re-use and scalability to reduce development cost and time-to-market. Rich feature set paired to high performance core allows for maximum efficiency in motor control and power conversion applications.

PSOC™ Connect™



Combining the most advanced MCU and wireless capabilities into a single package and leveraging advanced protection features and security architecture.

PSOC™ 6 Family



Proven balance between performance and low power, with security features and capabilities that enable OEMs to configure security for a myriad of use cases.

Copyright © Infineon Technologies AG 2026. All rights reserved.

Infineon PSOC MCUs Available in Four Edge Protect Categories (EPC) Providing the Right CRA Fit for OEMs

Edge Protect Category (EPC) #		EPC 1	EPC 2	EPC 3	EPC 4
Definition and Compliance		Minimum ICW MCU requirements PSA L1	Additional wireless connectivity security services PSA L2	Hardened accelerated crypto and fault, glitch mitigation PSA L3	Hardware isolated, lockstep Secure Enclave (SE) PSA3 + L4 iSE
Features	CRA support	✓ **Important Class 1**	✓ **Important Class 2**	✓ **Important Class 2**	✓ **Important Class 2**
	Cryptography (PQC support staring ’25)	✓ Accelerated	✓ Accelerated	✓ Hardened Accelerated	✓ Advanced Accelerated
	Secured boot	✓	✓	✓	✓
	Secured FW update	✓	✓	✓	✓
	Processing isolation	✓	✓	✓	✓
	Physical fault attack mitigation	✓ Boot-time	✓ Boot-time	✓ Boot-time/Run-time	✓ Boot-time/Run-time
	Prebuilt security stack available (TF-M)		✓	✓	✓
	Fault sensor management system			✓	✓
	DICE support for SPDM			✓ DICE Ready	✓
	Hardware isolated secure enclave (AVA.VAN.4)				✓

Edge Protect Categories were created with a focus on:

- **Global regulations (e.g. CRA)** – features, security certifications and response services to help customer comply and sell their products
- **Industry certifications (e.g. PSA)** – prevailing security certifications that customers care about and support OEM product certifications
- **Customer use cases and feedback** – application-based threat modeling for IoT device and device uses and direct customer learning
- **Differentiation** – leveraging our embedded security brand, IP and expertise to drive embedded-security leadership

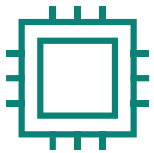
Copyright © Infineon Technologies AG 2026. All rights reserved.

How Infineon‘s PSOC MCUs can help with CRA compliance



- **Security-by-design:** Infineon’s PSOC MCUs have this as a core requirement
- **Keys and certificates** provisioned at Infineon's secured, Common Criteria-certified site

---



- **Security solutions for CRA compliance:** best-fit secured MCUs with complete documentation, certifications (PSA L1-L4) and Product Security Incident Response Team (PSIRT) already in place
- **Software tools:** Infineon's software tools and development platforms facilitate secured development, such as ModusToolbox™, Edge Protect Security Suite, and full multi-format SBOM available on request
- **Third-party certification:** independent evaluation and certification for standards (PSA-certified and SESIP)
- **Security lifecycle support for manufacturers:** to address the full product lifecycle, incl. risk assessment, vulnerability management, and reporting.
- **Evaluation platforms:** providing evaluation boards, reference designs, and security software (boot, FW updates, TF- stack)



- **Active in EU CRA standardizations**: contributing and leading EU standardization working groups in CENELEC
- **Decades-long expertise:** knowledge of regulatory requirements and variance of CRA compliance requirements
- **Training support:** Infineon provides resources like webinars to help customers understand and prepare for CRA
- **Implementation collaterals:** security-specific resources, such as, product documentation, security guidance manuals

Copyright © Infineon Technologies AG 2026. All rights reserved.

EU CRA Mandates SBOM: A Compliance Requirements



Purpose of SBOM

- **Vulnerability Management**
  - ✓ Quickly identify whether affected libraries
  - ✓ Components are used when new CVEs are disclosed.
- **Supply Chain Security**
  - ✓ Detect risks and attack paths from open-source or third-party components.
- **License Compliance**
  - ✓ Identify license conflicts early and reduce legal risks.
- **Transparency & Trust**
  - ✓ Provide visibility of software components to customers
  - ✓ Partners and support regulatory compliance.
- **Faster Incident Response**
  - ✓ Accelerate impact analysis and reduce remediation time (MTTR).
- **Standards Compliance**
  - ✓ Support industry SBOM formats such as Cyclone DX and SPDX format.

Copyright © Infineon Technologies AG 2026. All rights reserved.

Black Duck: SW for security, quality, SBOM and risk management

Infineon uses Black Duck as the standard tool for FOSS compliance, integrated through EDEN's containerized setup. Black Duck helps identify security, quality, and license compliance risks in open-source and third-party software by generating an accurate Bill of Materials (BoM) using its extensive component database.

Some key benefits:

- Multi-level scans
- Support for build tools and package manager files
- Easy to use UI
- Integrable to the existing CI pipelines
- Black Duck server hosted on-premise so on code goes outside Infineon
- Meet ISO26262
- Supports Cyclone DX and SPDX format

Copyright © Infineon Technologies AG 2026. All rights reserved.



In conclusion...

Public

CRA Standards are still in development and will have a profound effect globally once they come into force

- Risk assessment is the foundation, not an afterthought
- Don't start from a blank page, reuse trusted supplier evidence
- Infineon supports your CRA compliance journey with its certified security solutions



Copyright © Infineon Technologies AG 2026. All rights reserved.

Infineon's CRA Training Resources

Cyber Resilience Act (CRA): Foundations of Secure Solutions

Distribution FAE Certification Program (Silver)



Gain a comprehensive understanding of the EU Cyber Resilience Act and learn how to enable CRA compliance with Infineon's secure solutions, including SEMPER™, Secure NOR Flash, OPTIGA™ TPM, and USB Portfolio. This certification program covers the fundamentals of Infineon's security products and ModusToolbox™, providing a solid foundation for developing secure applications.

This certification program is made up of 2 sections:

1. MANDATORY courses offering you information related to the topic.
2. MANDATORY assessment
   - This assessment will validate your knowledge related to the online courses that make up this certification program.
   - The assessment contains 10 questions with a minimum passing grade of 80%.
   - The assessment can be repeated if you do not achieve the minimum passing grade on the first attempt.

Introducing the EU Cyber Resilience Act (CRA): a short training for C-level/management



Watch our training video to gain a comprehensive understanding of the EU Cyber Resilience Act and learn how to integrate its requirements into your business strategy, for a more secured and future ready organization

Copyright © Infineon Technologies AG 2026. All rights reserved.

Infineon's security products mapping across CRA product categories*

CRA categories	Default: "Unclassified"	Important: "Class I"	Important: "Class II"	Critical: Products
Class Specification	**Approximately 90% of products fall into this category**, which has a lower risk profile compared to other categories.	These are the products that present a higher cybersecurity risk (in terms of its intensity and ability to damage the health, security, or safety of users of such products) and should undergo a stricter conformity assessment procedure. **Class II** products hold a **higher level of criticality** and are thus subject to more stringent compliance measures, including **assessment by external third parties.**		These products have **cybersecurity-related functionality** that poses **a significant risk of adverse effects**, potentially disrupting or damaging multiple digital products.
Conformance	**Self assessment** Manufacturers can use Module A (internal control) to certify compliance rather than needing a third-party auditor	**Harmonized Standard (hEN)**** Manufacturers shall use hEN if self-assessment or 3rd party assessment to demonstrate that products comply with an EU legislation (e.g. EN 50765).	**Harmonized Standard (hEN)** and 3rd party assessment** Manufacturers shall use 3rd party assessment to demonstrate that products comply with an EU legislation	**EUCC** – European Cybersecurity Certification** Developed by ENISA to create a framework to certify products with digital elements meet the essential requirements of the CRA. **EN50764**[1] – standard for smart cards and eSE platforms.
Infineon products enabling CRA	**MCU** – PSOC™3 – PSOC™4 / BLE – PSOC™5 **Wi-Fi** – CYW43022 – CYW43012 – CYW4373E – CYW5459x – CYW43907/53907 **BTBLE** – 2070x/89072 – 20719/20721 – 20819/20820/89820 – 20736/20737 – 20835 – 30739	**MCU** – PSOC™ 61/62/63 with BLE 20829 – WiFi6 IoT Combo – PSOC™ Edge8x – PSOC™ with BLE – PSOC™ Control C3 – WiFi6 Auto Combo **Wi-Fi** – AIROC™ CYW5551x – AIROC™ CYW5557x **Wi-Fi MCU** – AIROC™ CYW5591x – PSW31xx WiFi/BT MCU – PSB3xxx BT MCU **Secure Memory** – SEMPER™ Secure	**MCU (Tamper-resistant MCUs)** – PSOC™ Edge8x **Security controllers** – OPTIGA™ Trust M std. – OPTIGA™ Trust MTR – OPTIGA™ Trust M – Express – OPTIGA™ Authenticate	**Secure Elements (eSE)**[2] – OPTIGA™ TPM (Common Criteria certified) – OPTIGA™ Connect – SECORA™

***Please note that the table is indicative and based on preliminary guidance;** it is subject to changes based on development of CRA harmonized standards, CRA implementation Acts, and any EU Commission- or ENISA-issued CRA guidance.

**Kindly note that the information provided here is intended for informational purposes only and does not constitute legal advice. The official text of the CRA supersedes the explanations provided here.

1 Until the EU Commission issues Delegated Acts allowing or requiring EUCC certification, Critical products must follow Class II assessment (Module B+C or H) and apply standards such as EN 50764

2 CRA requirements can be fulfilled with many MCUs and a discrete Secure Element can make the process easier and more efficient.

Copyright © Infineon Technologies AG 2026. All rights reserved.

Visit Infineon's CRA webpage
for more resources
and FAQs on CRA





Questions & Answers

Scan the QR code and please use this email R-IFX-SecurityG2M@infineon.com to ask your questions.

Public


Infineon