European Union

Cyber Resilience Act
How ST helps comply

Understanding the CRA

What is the Cyber Resilience Act (CRA)?

First EU legislation for mandatory cybersecurity requirements

Applies to all products with digital elements sold in the EU market that can connect directly or indirectly to another device or network

Covers hardware and software throughout the entire product life cycle

CRA compliance is a journey

Standards for facilitating compliance are still being developed.

They include 3 horizontal standards (aligned with Annex I Essential Requirements) and 35 vertical standards (for Important/Critical product categories), with deliverables expected by Q4 2026.

Conformity framework is still under development.

The notification of conformity assessment bodies will only start in June 2026. Manufacturers will then be able to start working with a Notified Body to put in place the steps to reach conformity

Is your business subject to CRA compliance?

The CRA applies to all products with digital elements

- that can connect directly or indirectly to another device or network
- sold in the EU market, regardless of manufacturer location
- Both final products and components placed separately on the market

Hardware products

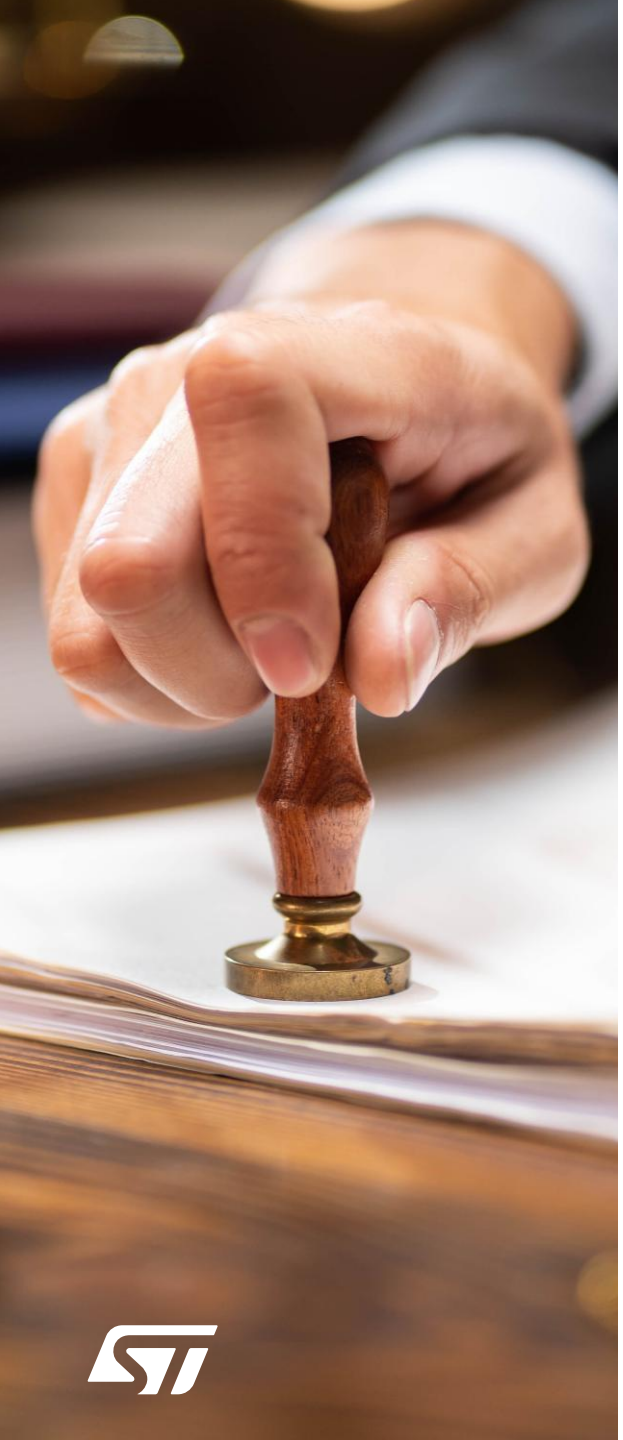
smartphones, IoT devices, smart home products, smart meters, smartcards, routers, switches…

Software products

Firmware, operating systems, mobile apps, desktop applications, video games…

Product exclusion

CRA avoids overlap with existing vertical cybersecurity regulations such as Medical devices, aviation equipment, automotive systems, marine equipment. Subcomponents of these end-products sold separately may still fall within the scope of CRA.



What’s the timeline for CRA compliance?

December 11, 2027
Full compliance enforcement
All products must meet essential requirements

September 11, 2026
Reporting obligations begin
24h & 72-hour vulnerability reporting required

June 11, 2026
Framework for Notified Bodies operational

December 10, 2024
Publication of the CRA final text

Why manufacturers need to act today.

- Non-compliant products banned from EU market
- Fines up to €15M or 2.5% of global annual turnover for core security failure (e.g. security-by-design, vulnerability management)
- up to €10M or 2% for documentation/reporting issues.

CRA compliance
What are the obligations for manufacturers?

Products	• Manufacturer shall conduct a **product risk assessment** • Products shall be designed, developed, and produced to ensure an **appropriate level of cybersecurity** based on the risks (Annex I Part I)
Vulnerabilities	• Manufacturers shall set up processes and practices to **handle vulnerabilities** (Annex I Part II) • Manufacturers shall **notify authorities** about actively exploited vulnerabilities and severe incidents
Conformity	• Products shall meet essential requirements through **self or third-party assessment** in line with the product categories • Manufacturer shall issue an **EU declaration of conformity & affix the CE marking**
Maintenance	Manufacturers shall maintain a **support period of at least 5 years** after the last sale of the product & **security updates for minimum 10 years**

CRA product categories & conformity assessment

Product category	Default products & open-source	Important products Class I	Important products Class II	Critical products
Conformity assessment procedures	Self-assessment			
	Self-assessment only if against Harmonized standard(s)			
	Third party - **product by product** assessment			
	Third party - **process** assessment: **Full quality assurance**			
	Third party – **EUCC** (EU Common Criteria) certificate			

ST is targeting conformity assessment based on **full quality assurance** to cover its products compliancy in addition to case-by-case product certification

How ST helps comply with the CRA

Which ST products are impacted by the CRA?

All ST products with a digital element and the ST-supplied software for these products.

Product type	CRA compliance
Dedicated automotive ICs	Automotive MCU, and some smart products
Analog, industrial & power conversion ICs	Smart analog / power management products
GP MCU & MPU, Wireless solutions, secure MCU, EEPROM	MCUs & MPUs, secure products, and wireless solutions
MEMS & optical sensing solutions	MEMS and Imaging products with digital processing embedded
ASICs based on ST proprietary technologies	Depending on functionality & customer requests
Discrete & power transistors	Not applicable

CRA compliance
Why ST is the right partner

We adapt **product development and life cycle** processes in alignment with the CRA.

As the CRA standards continue to evolve, we **closely follow developments and participate in standardization** and industry working groups.

We have a **long-standing security expertise**, established certifications, and proven proactive vulnerability management processes (ISO/IEC 29147, 30111)

30+ years of expertise with continuous innovation in security

Advanced secure technologies

- Post-quantum cryptography, secure provisioning, secure enclave
- First NIST ESV RNG certificate for SP800-90B
- First TEE turnkey solution with SESIP3 with STM32Trust
- Highest number of PSA & SESIP certificates in the industry
- First SESIP3 MCU with “Physical attacker resistance”

Securing a wide range of applications

- Banking & ID
- Brand protection and computer
- Secure mobile transactions
- Secure application digitalization
- IoT & industrial
- Automotive

About ST process-level and product certifications

Existing certifications

- Security certifications
- Common Criteria (EUCC) (ISO/IEC 15408): security evaluation methodology
- SESIP (EN 17927:2023): IoT platform security evaluation
- PSA Certified: Arm Platform Security Architecture certification
- EMVCo
- Process Certifications
- ISO 9001
- ISO/IEC 27001 (Information Security Management System)
- ISO/SAE 21434 (Automotive cybersecurity)
- TISAX (Automotive cybersecurity)

Why process-level certification?

Efficiency: Products under certified processes automatically covered

Consistency: Uniform security practices <across product lines

Agility: Faster time-to-market for new products

Proven approach: Aligned with key standards

Other processes followed (without certification)

- ISO/IEC 29147 (vulnerability disclosure)
- ISO/IEC 30111 (vulnerability handling)

ST is targeting Conformity assessment, based on **full quality assurance (module H)** to cover its products compliancy to CRA

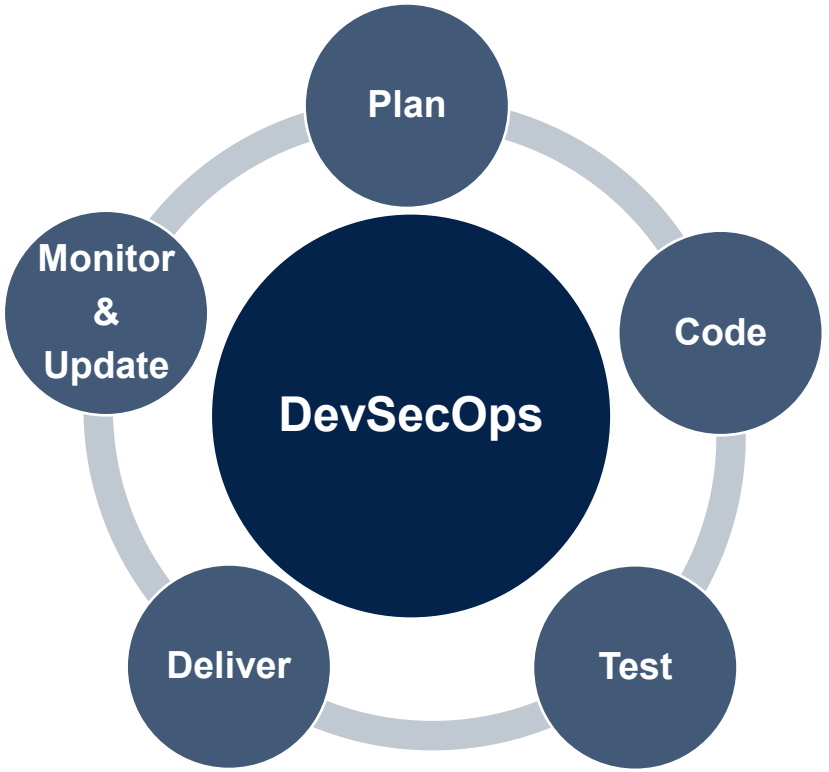
ST’s approach to security is based on DevSecOps

DevSecOps stands for development, security, and operations

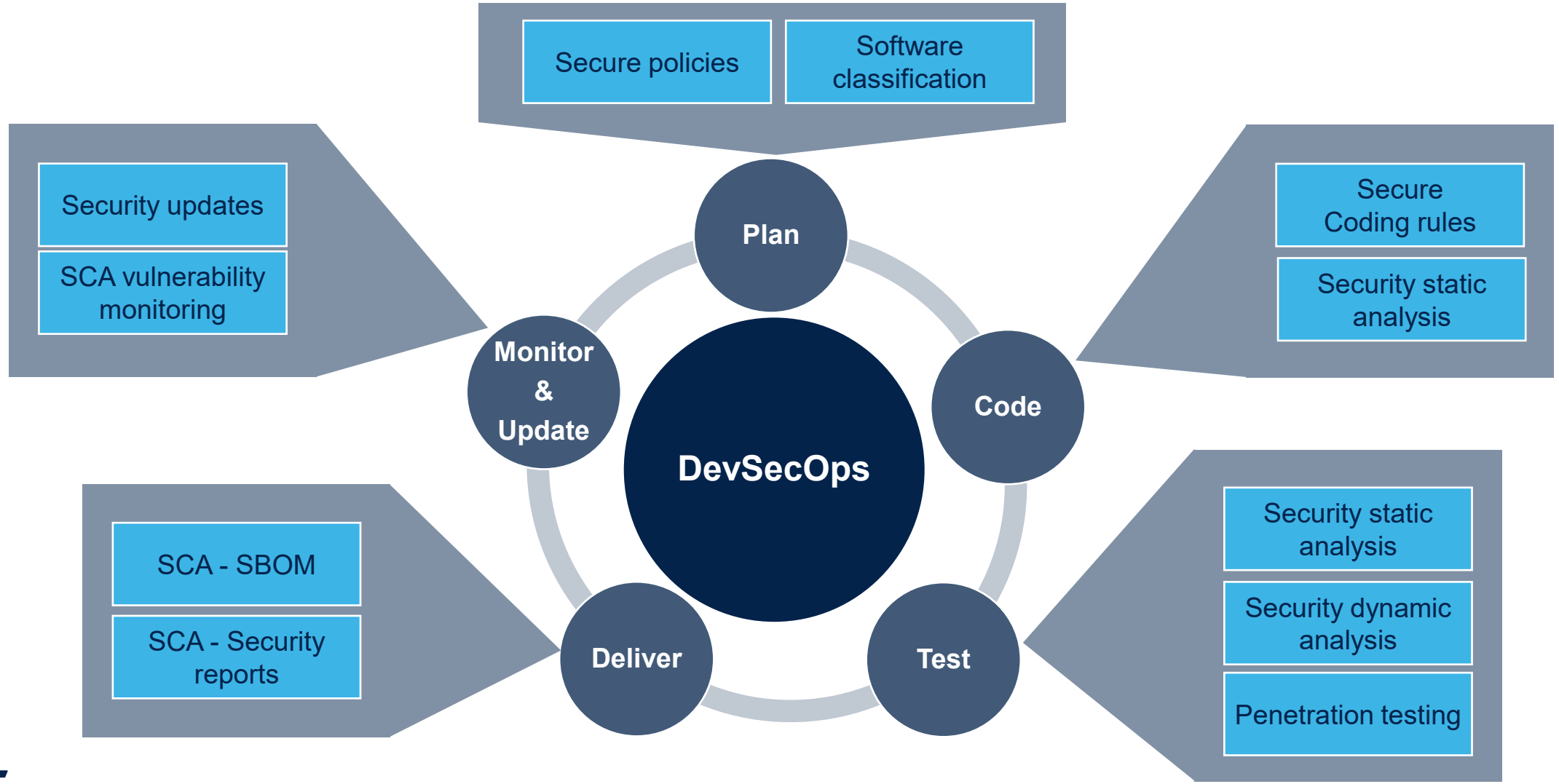
DevSecOps embeds security throughout the **entire software development life cycle** rather than treating it as a final checkpoint.

By integrating security practices into development and operations from the outset, **organizations reduce the likelihood of vulnerabilities** that reach production and encourage broader sharing of security responsibilities within teams

This proactive approach leverages automation and cross-functional collaboration to help **identify issues earlier,** when they are typically simpler and less costly to address



DevSecOps
How ST implements secure software development flow



ST’s approach with DevSecOps

By **integrating security** seamlessly into development and operations, DevSecOps supports ST in addressing CRA compliance more efficiently, reducing risks, and **delivering more secure products faster**.

CRA requirements	How DevSecOps addresses this
Secure development life cycle	Shift-left security, early vulnerability detection
Security testing & vulnerability management	Automated continuous security testing and scanning
Security across operations	Policy enforcement automation, continuous monitoring
Risk management assessment	Real-time risk visibility, integrated incident response
Security by design	Collaborative secure architecture and threat modeling
Ownership of vulnerabilities	Shared responsibility, integrated PSIRT workflows
Compliance updates	Agile pipeline updates, automated compliance checks

PSIRT
Product security incident response team

PSIRT is a corporate approach

Flaw reporting procedure follows security standards

- ISO/IEC 29147 : Vulnerability Disclosure
- ISO/IEC 30111: Vulnerability Handling Processes

Mandatory to pass security certifications like

- Arm PSA / ISO21434
- Global Platform SESIP

Part of SESIP3 certification target

- Flaw remediation process

Learn more
or report here.
st.com/PSIRT

CRA resources to keep you moving

Where can I find general information on CRA regulation?

Government resources

- European Community law webpage for information on official EU law documentation
- Current official version of REGULATION (EU) 2024/2847
- Some information on the law applicability Cyber Resilience Act | Shaping Europe's digital future
- Official European Union FAQ
- Visit the ENISA web portal to get the latest news and updates
- Cyber Resilience Act Requirements Standards Mapping is an interesting document available from ENISA that will evolve overtime

ST resources on CRA & RED

Useful resources

Security Wiki - Deep dive on CRA
https://wiki.st.com/stm32mcu/wiki/Security:Deep_dive_on_CRA

Wiki covering CRA requirement and product classification

Security: Q&A for CRA

https://wiki.st.com/stm32mcu/wiki/Security:Q%26A_for_CRA

Q&A for CRA

Webinar: Navigate new European security regulations with STM32Trust (part 1) – January 2025
https://content.st.com/new-european-security-regulations-with-stm32trust.html

RED and CRA scope and purpose. How ST security solutions enable compliance. Main compliance challenges, STM32Trust ecosystem overview

Webinar: Simplifying compliance with European security regulations (part 2) – February 2025
https://content.st.com/new-european-security-regulations-with-stm32trust-emea.html **topics covered:**

Recap of RED and CRA overview, risk assessment and countermeasure examples, IoT object use case with STM32Trust and STSAFE, Common security threats from IoT perspective)

Navigate new EU security regulations with STM32 wireless solutions

https://content.st.com/stm32-wireless-solutions-for-security-regulations.html

Understand the RED delegated act (DA) and harmonized standard EN-18031 for STM32 product certification requirements. Practical walkthrough: applying security using TrustZone®, secure boot, and FOTA implementation on STM32WBA for customer applications

ST resources on CRA & RED

Useful resources

Developing cyber-resilient railway components - Whitepaper

https://content.st.com/whitepaper-cyber-resilience-railway-components-z11-6366.html

Whitepaper outlines a framework for developing secure railway systems based on the IEC 62443 standard series. Highlights how ST's STM32 MCU/MPUs and the STM32Trust security framework provide a robust foundation for achieving compliance with cybersecurity regulations.

Navigate new EU security regulations (community post) - August, 2025
https://community.st.com/t5/developer-news/navigate-new-eu-security-regulations-with-st-solutions/ba-p/825228

Community article explaining CRA and RED requirements, ST's compliance approach, certified security solutions (SESIP, PSA), vulnerability management, and secure development life cycle.

New IoT security standards whitepaper (SESIP Level 3)
https://content.st.com/whitepaper-understanding-sesip-certification-for-microcontrollers-z11-5157.html
Importance of SESIP 3 certification for IoT manufacturers, Compliance, security, and scalability challenges, streamlining RED, and CRA compliance with SESIP Level 3 certified MCU, How STM32Trust provides multilevel security strategy, reducing complexity and costs of certification processes

Security Wiki - Deep dive on RED
https://wiki.st.com/stm32mcu/wiki/Security:Deep_dive_on_RED
Wiki covering RED requirements

Security: Q&A for RED
https://wiki.st.com/stm32mcu/wiki/Security:Q%26A_for_RED
Q&A on RED requirements

ST security-related resources

Useful resources

ST PSIRT (Product security incident response team)
https://www.st.com/content/st_com/en/security/report-vulnerabilities.html

Central page for reporting security vulnerabilities, accessing security advisories, and understanding ST's vulnerability management process.
Contact: psirt@st.com

Embedded security solutions & products
https://www.st.com/en/applications/embedded-security.html

Overview of ST's security portfolio, including STM32Trust, STSECURE products, secure elements, certifications (PSA, SESIP, Common Criteria), and post-quantum cryptography program.

STM32Trust security framework
https://www.st.com/content/st_com/en/ecosystems/stm32trust.html

Detailed information about STM32Trust's 12 security functions for MCUs and MPUs, supporting certifications (PSA, SESIP, Common Criteria EAL5+), and compliance with security standards.

STSECURE - Secure MCU portfolio
https://www.st.com/en/secure-mcus.html

Complete portfolio of secure microcontrollers for payment, identity, authentication, IoT, and automotive applications.

Secure hardware platforms
URL: https://www.st.com/en/secure-mcus/secure-hardware-platforms.html

Details on ST secure microcontrollers, Common Criteria certifications (EAL6+), EMVCo compliance, and hardware security features.

ST security-related resources

Useful resources

STM32 software security policies Q&A

https://wiki.st.com/stm32mcu/wiki/Security:STM32_Software_security_policies_Q%26A

Q&A on STM32 security policies

STM32Trust software security policies

Security: STM32Trust software security policies - stm32mcu

Wiki on STM32Trust security policies

Resources from ST partners

Useful resources

Avnet Silica - Helping you comply with the EU Cyber Resilience Act
https://my.avnet.com/silica/solutions/security-services/secure-device-management-provisioning/cyber-resilience-act/
Focus on: STM32H573 device with Arm® Cortex® M33, SESIP Level 3 compliant Secure Manager root of trust

EBV factory automation techdays - CRA session
https://ebvtechdays.com/stmicroelectronics/sessions/radio-equipment-directive-cyber-resilience-act-impact-on-your-mcu-related-cyber-security-applications
Conference session on RED and CRA impact on MCU-related cybersecurity applications.

Annex & glossary

Glossary
CRA-specific terms

CE marking

A mandatory conformity marking for products sold in the European Economic Area (EEA). Under CRA, the CE mark indicates the product meets cybersecurity requirements.

Conformity assessment

The process of demonstrating that a product meets CRA requirements. Can be self-assessment (manufacturer evaluates their own product) or third-party assessment (independent body verifies compliance).

Essential cybersecurity requirements

The mandatory security standards listed in CRA Annex I that products must meet. Split into Part I (product properties) and Part II (vulnerability handling).

Market surveillance authority

Government bodies in each EU member state responsible for monitoring and enforcing CRA compliance in their market.

Products with Digital Elements (PDE)

Any hardware or software product whose intended use includes a direct or indirect connection to a device or network. Examples: smartphones, IoT devices, routers, smart home devices, connected cars, industrial controllers.

Support period

The time during which manufacturers must provide security updates and support for a product after it's placed on the market.

Glossary
Security architecture terms

Attack Surface

All the points where an unauthorized user could try to enter or extract data from a system. Smaller attack surface = fewer vulnerabilities. Like having fewer doors and windows in a building makes it easier to secure.

Hardware Security Module (HSM)

A dedicated physical computing device that safeguards and manages cryptographic keys and performs encryption operations. Think of it as a secure vault inside a chip.

Secure boot

A security feature ensuring that a device only runs software that is trusted and hasn't been tampered with. Like checking ID before allowing entry.

Secure by design

Building security into a product from the beginning of development rather than adding it later. Like designing a house with locks on doors rather than trying to add them after it's built.

Secure by default

Shipping products with security features already enabled and configured safely. Users don't need to be security experts to be protected.

Secure element

A tamper-resistant chip that securely stores sensitive data and runs security-critical applications. Like a safe within your computer.

Glossary
Vulnerability & threat terms

Denial of Service (DoS) Attack

An attack that makes a service unavailable by overwhelming it with traffic or requests. Like blocking a store entrance so customers can't get in.

Exploitable vulnerability

A vulnerability that attackers can actually use to cause harm. Not all vulnerabilities are easily exploitable.

Malware

Malicious software designed to harm, exploit, or compromise a system. Includes viruses, trojans, ransomware, etc.

Patch / security update

Software fixes released by manufacturers to address security vulnerabilities. Like repairs to fix security weaknesses.

Vulnerability

A weakness in software or hardware that could be exploited to compromise security. Like a crack in a door that could be pried open.

Zero-Day vulnerability

A security flaw that's discovered and exploited before the manufacturer knows about it or can fix it.

Glossary
Security management terms

Coordinated vulnerability disclosure

A process where security researchers privately report vulnerabilities to manufacturers, giving them time to fix issues before public announcement. Prevents attackers from learning about vulnerabilities before fixes are available.

CVE (Common vulnerabilities and exposures)

A standardized identifier for publicly known security vulnerabilities. Like a universal catalog number for security flaws.

PSIRT (Product security incident response team)

A dedicated team within a company that handles security vulnerability reports and coordinates responses. Like an emergency response team for cybersecurity.

SBOM (Software bill of materials)

A complete list of all software components, libraries, and dependencies in a product. Like an ingredients list for software - helps track what's inside and identify vulnerabilities.

Threat intelligence

Information about current and emerging cybersecurity threats. Helps organizations prepare for and defend against attacks.

Glossary
Certification & standards terms

Common Criteria (CC)

An international standard (ISO/IEC 15408) for computer security certification. Products are evaluated at different levels (EAL1-EAL7), with higher levels indicating more rigorous testing.

EAL (Evaluation Assurance Level)

The security assurance rating in Common Criteria certification. EAL1 is basic, EAL7 is highest. ST's secure elements achieve EAL5+ and EAL6+.

EMVCo

Global technical body managing specifications for payment cards and acceptance devices. EMV® certification is required for payment card products.

EUCC (EU Common Criteria)

European cybersecurity certification scheme based on Common Criteria, specifically for CRA compliance.

PSA (Platform Security Architecture)

A security framework defined by Arm for IoT devices, providing guidelines and certification for secure design.

SESIP (Security evaluation standard for IoT platforms)

A security evaluation standard from GlobalPlatform specifically designed for IoT devices and platforms.

Our technology starts with You

Find out more at www.st.com