Global Platform®

May 22, 2025

CRA for Device Makers

Applicability for Components, Devices, and Systems

Carlos Serratos
NXP – Security Certification Expert
GlobalPlatform – Chairman SESIP Ecosystem Adoption WG

globalplatform.org

Agenda

- What's the CRA
- CRA Principles
- CRA Conformance
- CRA & Automotive
- Key takeaways

What is the Cyber Resilience Act (CRA)

Scope: Europe

Goal: "*To harmonise cybersecurity requirements for products with digital elements in all Member States*"

Horizontal regulation, touching:

- RED
- NIS2 for critical infrastructure
- AI Act for AI
- eIDAS for wallets/eIDs
- GDPR for data protection
- Liability Act
- Safety Act
- Machinery Directive
- Cybersecurity Act

Mandatory for CE mark from December 2027:

Access to the EU market

Penalties:

For non-complying essential requirements, it can amount to **€15 million or 2.5% of the annual turnover**, whichever is higher.

Applicability

Finished products with digital elements (SW/HW), **except products that have an existing European regulation in place:**

- Ground Transportation
- Air transportation
- Medical for human and in-vitro diagnostic

Commercial Software

HW/SW subcomponents, including MCUs, MPUs, Crypto Processors and Secure Elements used in **ANY** application, including those above

CRA principles

If it’s ”smart”, maybe it is not

It applies to every “connected” vertical and application
(minus medical & automotive systems and vehicles)

CRA principles

If it's "smart", maybe it is not

It applies to every "connected" vertical and application
(minus medical & automotive systems and vehicles)

"Everything" is a potential backdoor

It applies to any HW and SW
End devices, components, and
remote services alike

CRA principles

If it's "smart", maybe it is not
It applies to every "connected" vertical and application
(minus medical & automotive systems and vehicles)

"Everything" is a potential backdoor
It applies to any HW and SW
End devices, components, and remote services alike

Risk first, and last
Documented risk-based decisions
User guidance
Secure technology and processes

CRA principles

If it's "smart", maybe it is not
It applies to every "connected" vertical and application
(minus medical & automotive systems and vehicles)

"Everything" is a potential backdoor
It applies to any HW and SW
End devices, components, and remote services alike

Risk first, and last
Documented risk-based decisions
User guidance
Secure technology and processes

Risk is contextual
Security problems might have several solutions (SOTA)

CRA principles

If it's "smart", maybe it is not
It applies to every "connected" vertical and application
(minus medical & automotive systems and vehicles)

"Everything" is a potential backdoor
It applies to any HW and SW
End devices, components, and remote services alike

Risk first, and last
Documented risk-based decisions
User guidance
Secure technology and processes

Security is not a one-off
Vulnerability management
Support period & Surveillance

Risk is contextual
Security problems might have several solutions (SOTA)

CRA principles

If it's "smart", maybe it is not
It applies to every "connected" vertical and application
(minus medical & automotive systems and vehicles)

"Everything" is a potential backdoor
It applies to any HW and SW
End devices, components, and remote services alike

Risk first, and last
Documented risk-based decisions
User guidance
Secure technology and processes

Security is not a one-off
Vulnerability management
Support period & Surveillance

Risk is contextual
Security problems might have several solutions (SOTA)

You can never be 100% sure
Secure supply chains,
Beyond secure products, secure suppliers

CRA principles

If it's "smart", maybe it is not
It applies to every "connected" vertical and application
(minus medical & automotive systems and vehicles)

"Everything" is a potential backdoor
It applies to any HW and SW
End devices, components, and remote services alike

Risk first, and last
Documented risk-based decisions
User guidance
Secure technology and processes

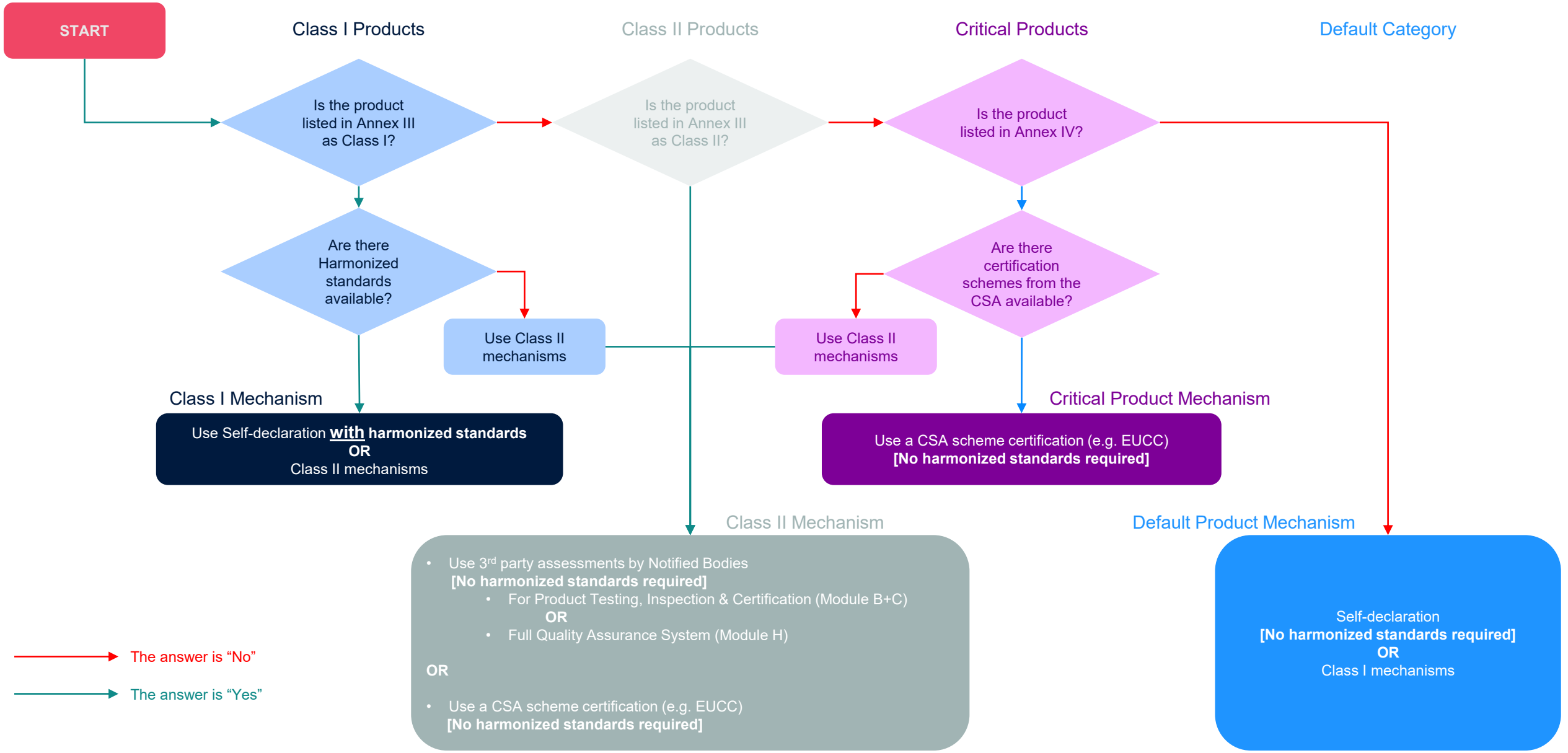
Security is not a one-off
Vulnerability management
Support period & Surveillance

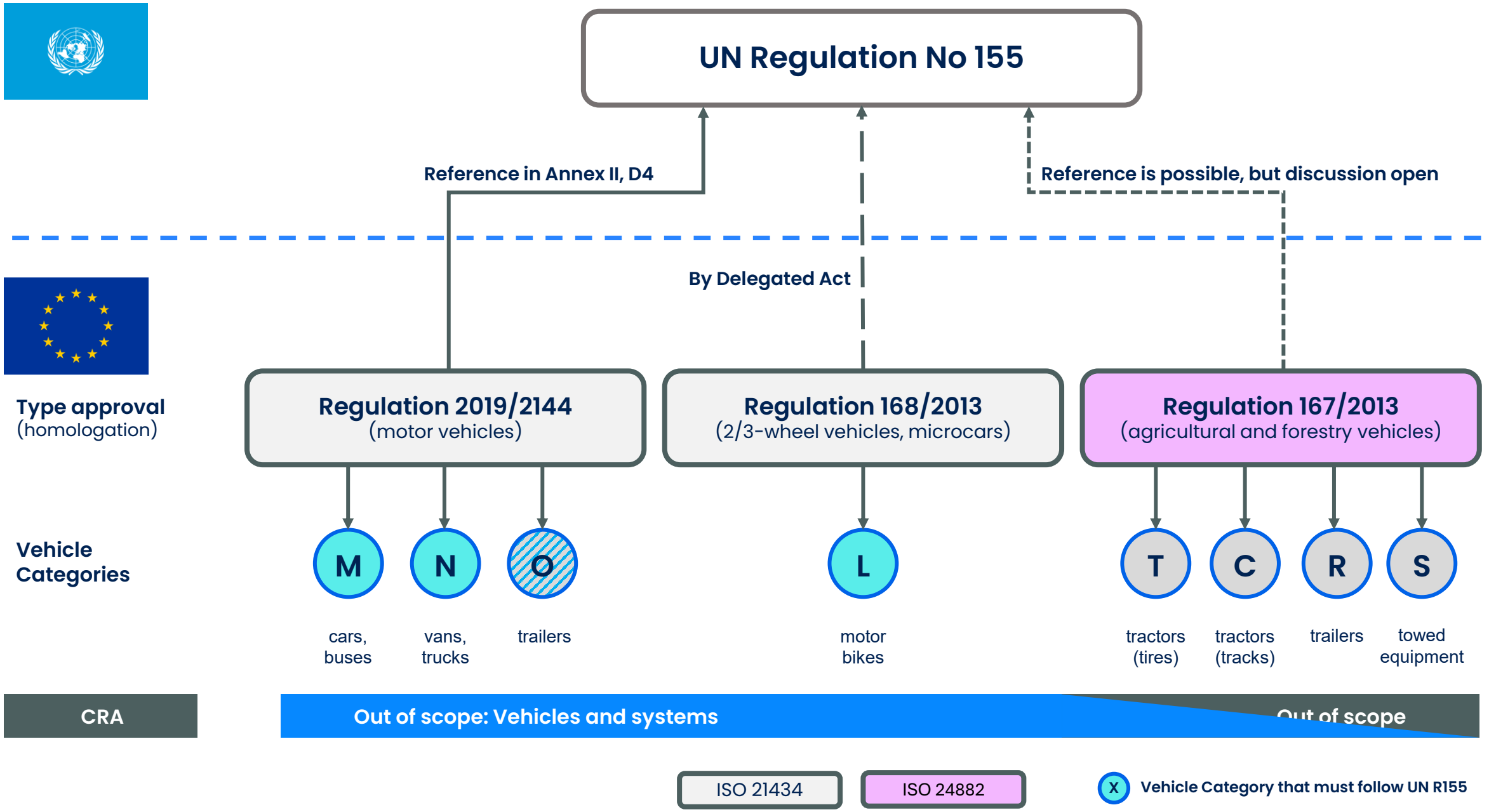
Risk is contextual
Security problems might have several solutions (SOTA)

Trust, and verify
Different conformance mechanisms for products based on impact

You can never be 100% sure
Secure supply chains,
Beyond secure products, secure suppliers

CRA Conformance mechanisms




UN Regulation No 155
Reference in Annex II, D4
Reference is possible, but discussion open
By Delegated Act
Type approval
(homologation)
Regulation 2019/2144
(motor vehicles)
Regulation 168/2013
(2/3-wheel vehicles, microcars)
Regulation 167/2013
(agricultural and forestry vehicles)
Vehicle Categories
M
N
O
L
T
C
R
S
cars, buses
vans, trucks
trailers
motor bikes
tractors (tires)
tractors (tracks)
trailers
towed equipment
CRA
Out of scope: Vehicles and systems
Out of scope
ISO 21434
ISO 24882
X
Vehicle Category that must follow UN R155

Global Platform®

The most important element from the CRA:
If there is something you need to remember…

- The CRA doesn't mandate compulsory or mandatory functionality
- Manufacturers "own" the risk, the obligation to mitigate the risk, and communicate it to the users
- The conformance Classes only represent the conformance mechanisms: there is no basic, minimum, or entry-level security, even in the default category
- The essential requirements are the baseline that needs to be addressed. It doesn't mean it needs to be implemented
  - What and how is implemented is up to the manufacturer but always, always, always: **risk-based (documented) decisions**

Global Platform®

The standard for secure digital services and devices

→globalplatform.org