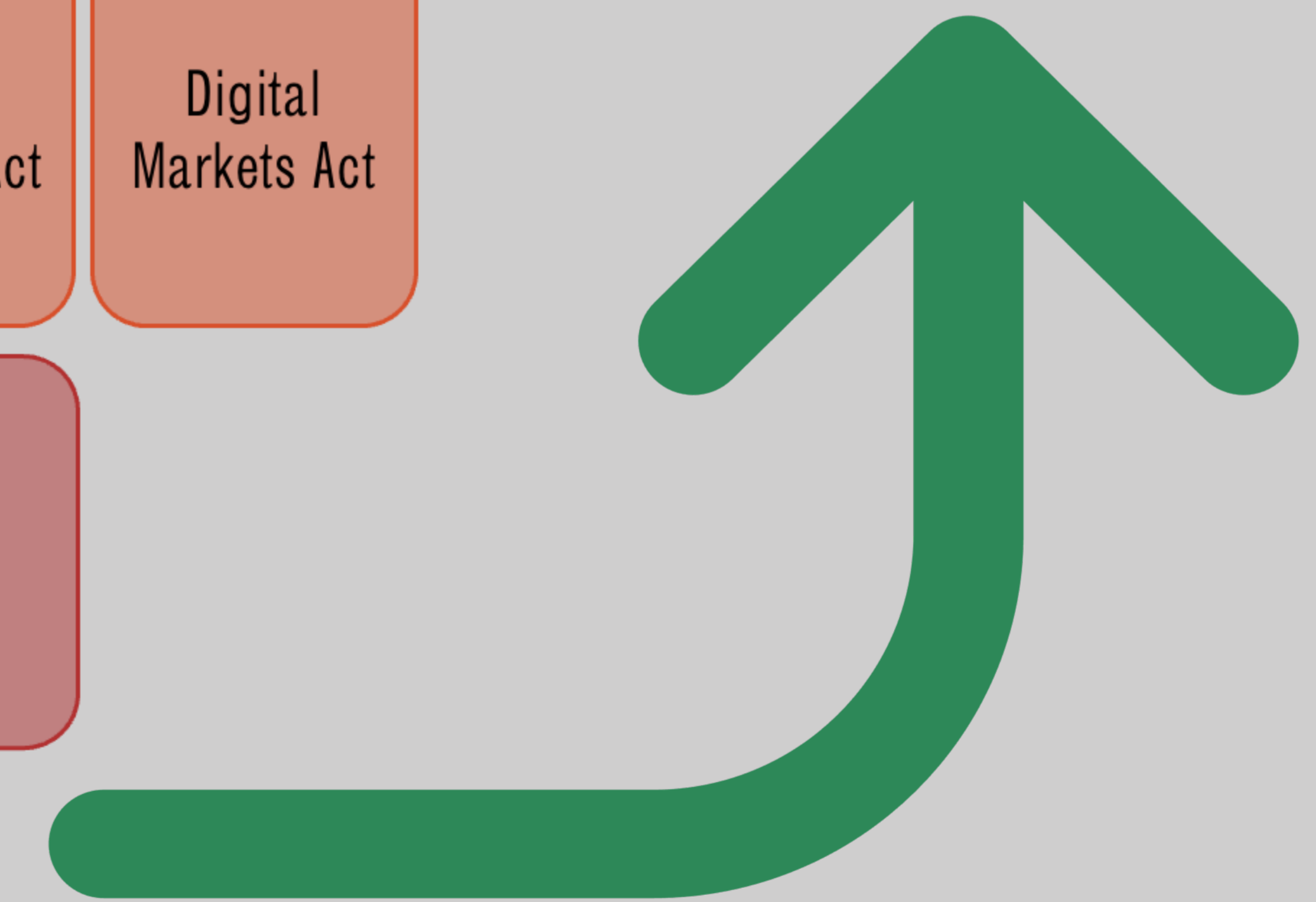
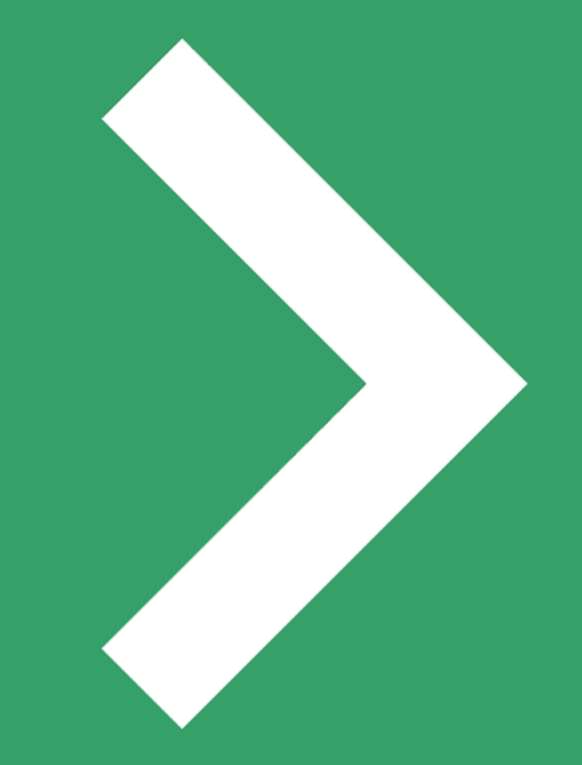


CRA

PROJECT
MOORE



CRA

IN A NUTSHELL

PROJECT
MOORE

Reasons for CRA

- Inadequate cybersecurity for connected products with digital elements.
- Insufficient security updates for ongoing protection.
- Limited user understanding and access to critical security information.

CRA key objectives

- Establishing boundary conditions for developing secure, connected products with digital elements (security by design).
- Ensuring security is maintained across the entire product life cycle
- Enabling users to securely operate products with digital elements.



WHAT?

KEY COMPONENTS

PROJECT
MOORE

Connected products with digital elements

soft/hardware product and its
remote data processing

solutions



Almost every IoT
product*

Almost all
software*

*Exceptions

⊖ Non-commercial software, incl.
free open source

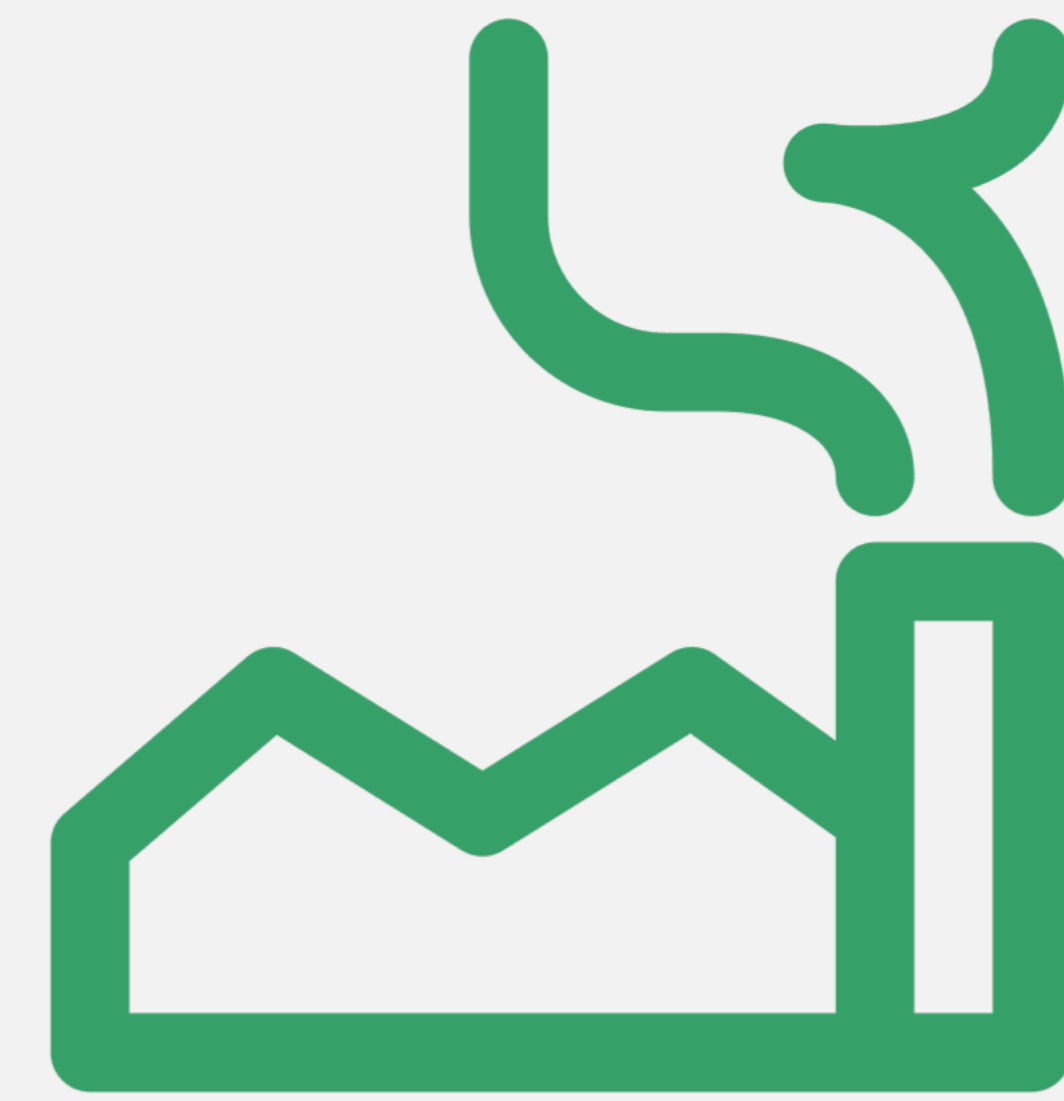
⊖ Software-as-a-Service (unless
provided as a remote data
processing solution)

⊖ Certain regulated or certified
products



WHO? ECONOMIC OPERATORS'

PROJECT
MOORE



Manufacturer*

Natural/legal person who...

Develops or manufactures products with digital elements

Or has them designed, developed, or manufactured

And markets them in the EU under its own trademark, whether for payment or free of charge.

*Most obligations apply to manufacturers



Importer

Imports products from outside the EU



Distributor

Makes products available without affecting properties



HOW?

1. SECURITY REQUIREMENTS

PROJECT
MOORE



Manufacturer

Security by design

- Ensure cybersecurity appropriate to identified risks
- Meet essential security requirements via risk assessment
- Be free of known vulnerabilities

Response to vulnerabilities

- Test, address, and document vulnerabilities
- Provide security updates for at least 5 years or product lifespan if shorter
- Inform and instruct users about vulnerabilities
- Have a responsible disclosure policy and contact

↓
Security by
design



Response to
vulnerabilities



HOW?

1. SECURITY REQUIREMENTS



Manufacturer

Accountability

- Conformity assessment essential security requirements
- Stricter rules important and critical products
- Create technical documentation

User information

- Ensure products include clear, understandable, and accessible user information and instructions



HOW?

2. SUPPLY CHAIN CONTROL

PROJECT
MOORE



Manufacturer*

- Security by design & response to vulnerabilities rules
- Accountability and user instructions
- Notification obligations

*See previous slides

+ Check on third party components



Distributor

- Duty of care
- Place only compliant products on market
- Compliance check
- Contact details
- Notification obligations

+ Check on importer & manufacturer



Importer

- Place only compliant products on market
- Compliance check
- Contact details
- Notification obligations

+ Check on manufacturer



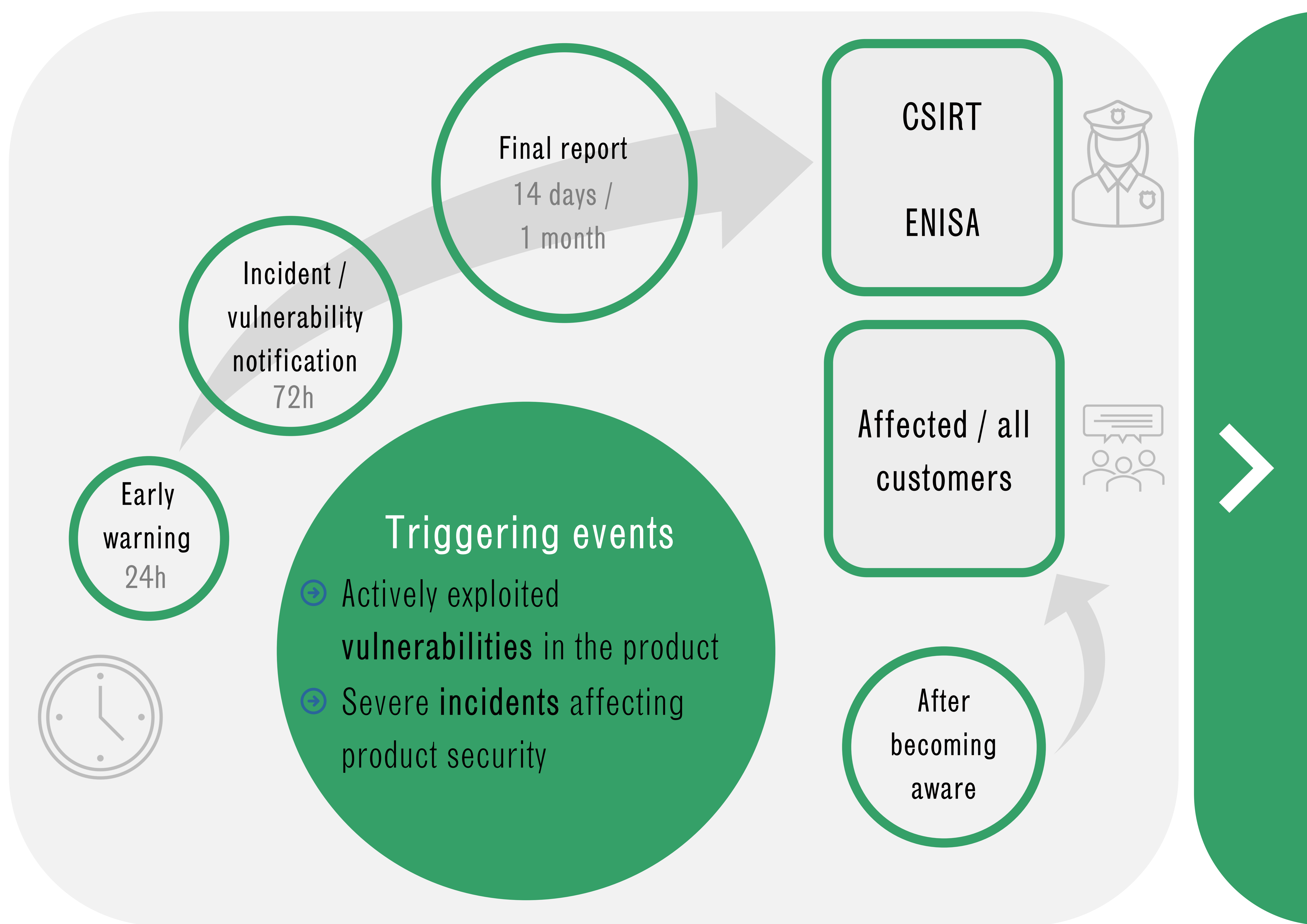
Third Party



HOW?

NOTIFICATION OBLIGATIONS

PROJECT MOORE



HOW?

ENFORCEMENT AND PENALTIES


PROJECT
MOORE



Sanctions*

 Fines up to €15 million or 2.5% of annual turnover
For violations of essential cybersecurity requirements,
conformity assessments, and reporting obligations.

 Fines up to €10 million or 2% of annual turnover
For breaches of other CRA rules.

 Fines up to €5 million or 1% of annual turnover
for providing incorrect, incomplete, or misleading
information.

*Other enforcement powers include recall of products



By Whom?

Member States designate
any existing or new
authority to a market
surveillance authority



WHEN?

KEY DEADLINES

PROJECT
MOORE



15 DEC 2020 Publication EU Cybersecurity strategy



15 SEP 2022 EC adopts CRA proposal



10 DEC 2024 CRA officially comes into force



11 SEP 2026 Reporting obligations manufacturers



11 DEC 2027 Main CRA provisions become applicable



**FOR MORE
CHECK [PROJECTMOORE.COM](https://projectmoore.com)**

**PROJECT
MOORE**