EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA SKILLS AD-HOC WORKING GROUP

MAPPING ECSF IN THE CONTEXT OF PRODUCT SECURITY

DR. JETZABEL MARITZA SERNA-OLVERA

20 | 11 | 2025

CONTENTS

- Introduction and rationale
- The product security skills mapping activity
- Manufacturer use case scenario
- Next steps

THE EMERGING NEED FOR ROBUST CYBERSECURITY IN PRODUCTS WITH DIGITAL ELEMENTS

REGULATORY OBLIGATIONS AND SYSTEMIC RISK CONSIDERATIONS

- **Connected devices increase systemic cyber risk**, impacting safety, economy, and society.
- Many products still show **low cybersecurity maturity;** vulnerabilities, weak updates, limited user awareness.
- The EU is enforcing **secure-by-design and lifecycle security** requirements across digital products.
- Manufacturers must prove **organizational capability and skilled staff** to manage cybersecurity risks across the value chain.
- Notified bodies must prove they are impartial, **competent**, and properly equipped to assess product cybersecurity.
- Market surveillance authorities need to ensure their inspectors and analysts are equally equipped to assess compliance, investigate cybersecurity incidents, and **understand the technical and regulatory underpinnings of product security**.

Mapping skills in product security context

MAPPING ECSF IN THE CONTEXT OF PRODUCT SECURITY

GENERAL ASPECTS

- Activity framed within the project: 'ENISA Cybersecurity Skills Framework (ECSF)'
- Focus on regulatory analysis for a better uptake of the ECSF
- Co-developed within the ECSF AHWG – "Product Security" Focus group

MAIN OBJECTIVE

- To map cybersecurity skills needs for the implementation of product security regulatory obligations, taking as reference the ECSF of ENISA.

SPECIFIC OBJECTIVES

- Demonstrate the ECSF's applicability to product security beyond traditional IT domains.
- Align product security competencies with EU regulatory, certification and industry requirements
- Support harmonized skills recognition and workforce development across key sectors e.g., consumer products, automotive, healthcare,

USE CASES AND INTENDED AUDIENCE

SCENARIOS

- Manufacturers
- Notified bodies
- Market surveillance authorities

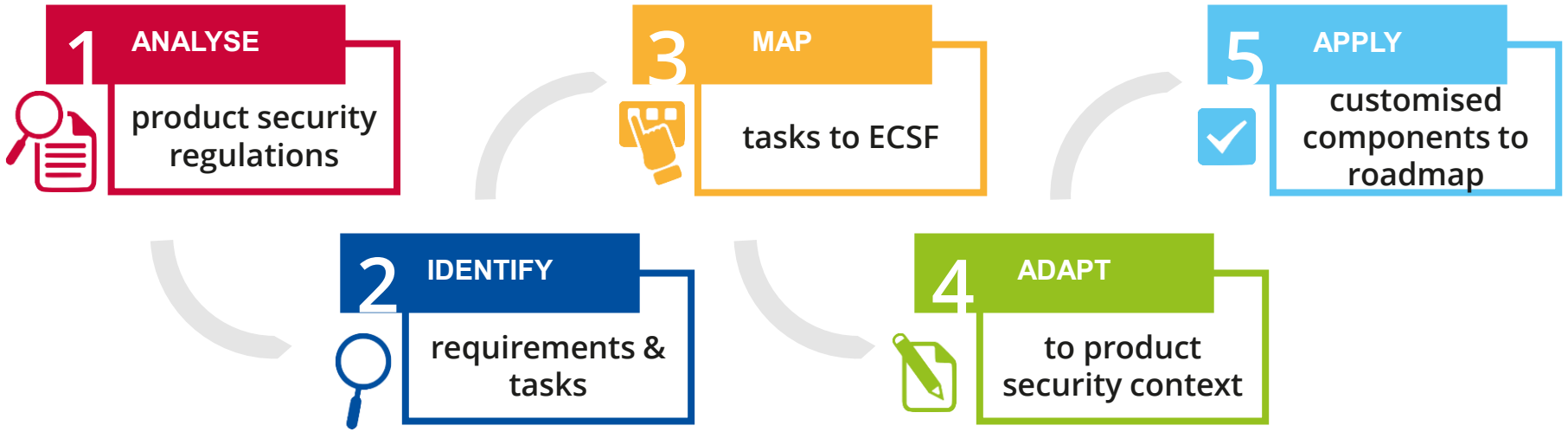
TARGET AUDIENCE

- Manufacturers and industry leaders
- Conformity assessment (notified) bodies
- Market surveillance authorities
- Cybersecurity professionals
- Academic and training providers
- Policy makers and regulators

Manufacturer use case scenario

METHODOLOGY

MANUFACTURER USE CASE SCENARIO



ANALYZED PRODUCT SECURITY REGULATIONS

Official Journal of the European Union — EN — L series

2024/2847 — 20.11.2024

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 October 2024

on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

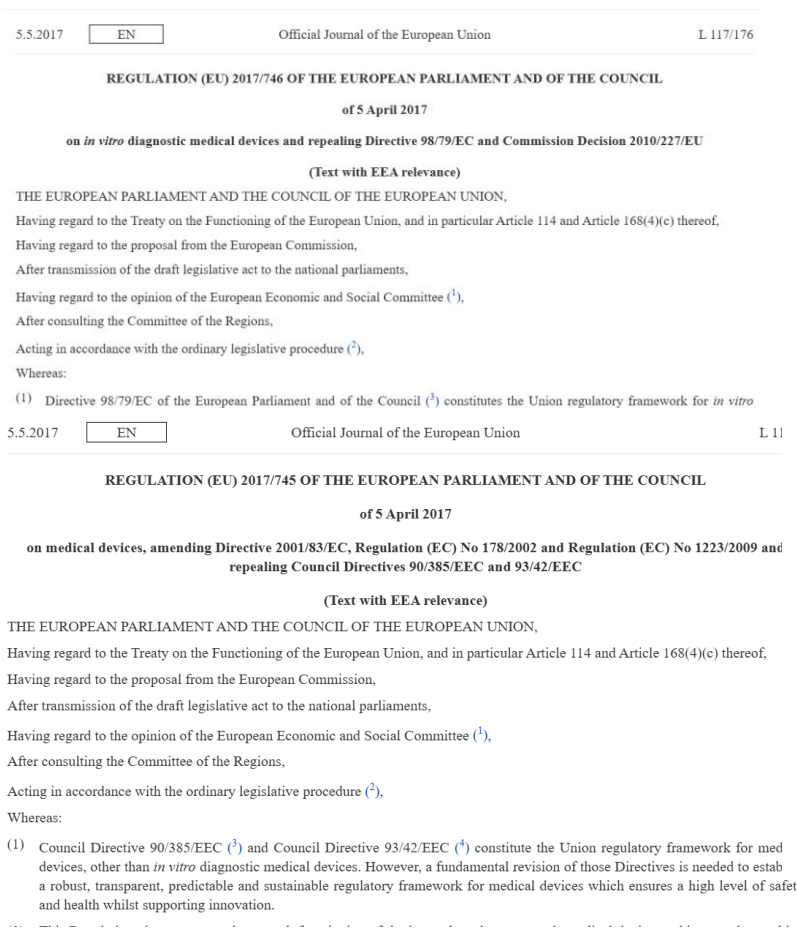
Having regard to the opinion of the European Economic and Social Committee [1],

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure [2],

Whereas:

(1) Cybersecurity is one of the key challenges for the Union. The number and variety of connected devices will rise exponentially in the coming years. Cyberattacks represent a matter of public interest as they have a critical impact not only on the Union's economy, but also on democracy as well as consumer safety and health. It is therefore necessary to strengthen the Union's approach to cybersecurity, address cyber resilience at Union level and improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market. Two major problems adding costs for users and society should be addressed: a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.



5.5.2017 — EN — Official Journal of the European Union — L 117/176

REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 5 April 2017

on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 and Article 168(4)(c) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee [1],

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure [2],

Whereas:

(1) Directive 98/79/EC of the European Parliament and of the Council [3] constitutes the Union regulatory framework for *in vitro*

5.5.2017 — EN — Official Journal of the European Union — L 11

REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 5 April 2017

on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 and Article 168(4)(c) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

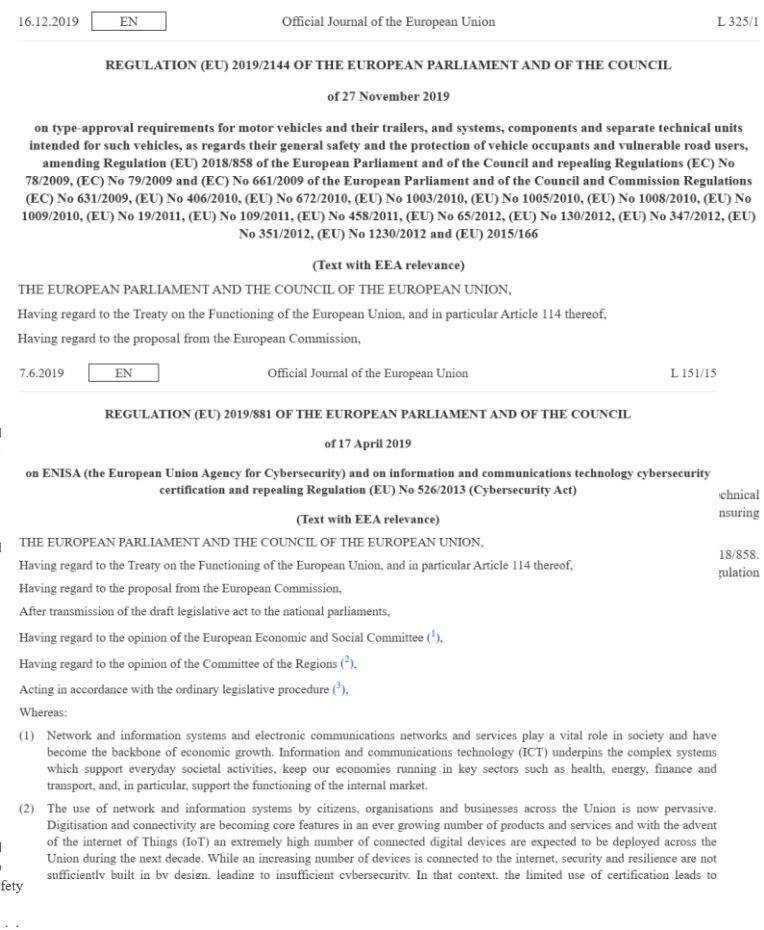
Having regard to the opinion of the European Economic and Social Committee [1],

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure [2],

Whereas:

(1) Council Directive 90/385/EEC [3] and Council Directive 93/42/EEC [4] constitute the Union regulatory framework for med devices, other than *in vitro* diagnostic medical devices. However, a fundamental revision of those Directives is needed to estab a robust, transparent, predictable and sustainable regulatory framework for medical devices which ensures a high level of safety and health whilst supporting innovation.



16.12.2019 — EN — Official Journal of the European Union — L 325/1

REGULATION (EU) 2019/2144 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 November 2019

on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

7.6.2019 — EN — Official Journal of the European Union — L 151/15

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 17 April 2019

on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee [1],

Having regard to the opinion of the Committee of the Regions [2],

Acting in accordance with the ordinary legislative procedure [3],

Whereas:

(1) Network and information systems and electronic communications networks and services play a vital role in society and have become the backbone of economic growth. Information and communications technology (ICT) underpins the complex systems which support everyday societal activities, keep our economies running in key sectors such as health, energy, finance and transport, and, in particular, support the functioning of the internal market.

(2) The use of network and information systems by citizens, organisations and businesses across the Union is now pervasive. Digitisation and connectivity are becoming core features in an ever growing number of products and services and with the advent of the internet of Things (IoT) an extremely high number of connected digital devices are expected to be deployed across the Union during the next decade. While an increasing number of devices is connected to the internet, security and resilience are not sufficiently built in by design, leading to insufficient cybersecurity. In that context, the limited use of certification leads to

Cybersecurity Act; Cyber Resilience Act; Regulation (EU) 2019/2144 UN R 155; Regulation (EU) 2017/745 and 2017/746

TASK IDENTIFICATION (EXAMPLE)

Reg. obligation	Main object	Task/requirements
	Manufacturer	**Maintain an up-to-date regulatory mapping aligning each product with applicable EU security frameworks and the appropriate conformity routes**
CRA Art 13	Manufacturer	Draft, approve, and maintain cybersecurity policies and procedures covering risk management, secure development, supply chain security, vulnerability handling, coordinated disclosure, incident response, and updates.
		Complete technical documentation and conformity evidence prior to placing the product on the market
		Plan and perform risk assessments for each product with digital elements, covering the entire lifecycle
		Update assessments continuously when products or environment change or new vulnerabilities/incidents arise
CRA Art 14	Manufacturer	Report actively exploited vulnerabilities and severe incidents to authorities and affected parties within the required timeframes.
CRA Art 18	Manufacturer	Cooperate with market surveillance authorities , providing access to data and documentation when requested.

MAP AND ADAPT (EXAMPLE)

Task	ECSF Task	Adapted ECSF role
Draft, approve, and maintain cybersecurity policies and procedures covering risk management, secure development, supply chain security, vulnerability handling, disclosure, incident response, and updates.	Prepare and present cybersecurity vision, strategies and policies for approval by senior management and ensure their execution	Chief Product Security Officer
Develop workforce competence by defining upskilling/re-skilling needs and rolling out training and awareness programs	Manage continuous cybersecurity capacity building	Chief Product Security Officer
Maintain an up-to-date regulatory mapping aligning each product with applicable EU security frameworks and the appropriate conformity routes	Identify and manage legal and regulatory requirements	Cyber Legal and Compliance Officer
Plan and perform risk assessments for each product with digital elements, covering the entire lifecycle.	Develop, maintain, report and communicate complete risk management cycle	Cyber Risk Manager

ROADMAP (SMALL AND MEDIUM-SIZED ENTERPRISES)

Establish governance & accountability

Identify skills gaps; upskill, reskill, outsource

Embed risk management and secure design

Verify and prepare for market

Strengthen operations & post market activities

Build continuous improvement and market trust

Next steps

NEXT STEPS AND STAKEHOLDER INVOLVEMENT

- Conduct internal review and feedback round within ENISA's ECSF AHWG.
- Engage Market Surveillance experts to develop use case scenario 3.
- Involve ENISA's Product Security Group for expert validation and alignment.
- Prepare the internal-only report based on consolidated feedback.

THANK YOU

QUESTIONS?

FOR MORE INFORMATION

ENISA EU SKILLS (euskills@enisa.europa.eu)

info@enisa.europa.eu

www.enisa.europa.eu