CRYPTO
Part of Fox-IT

Upcoming IT legislation – are you ready?

Ellen Wesselingh CCG

December 2024

Agenda

General aspects of information security:

1. Confidentiality, Integrity, Availability (CIA) – legislation adds Authenticity
2. Risk Management

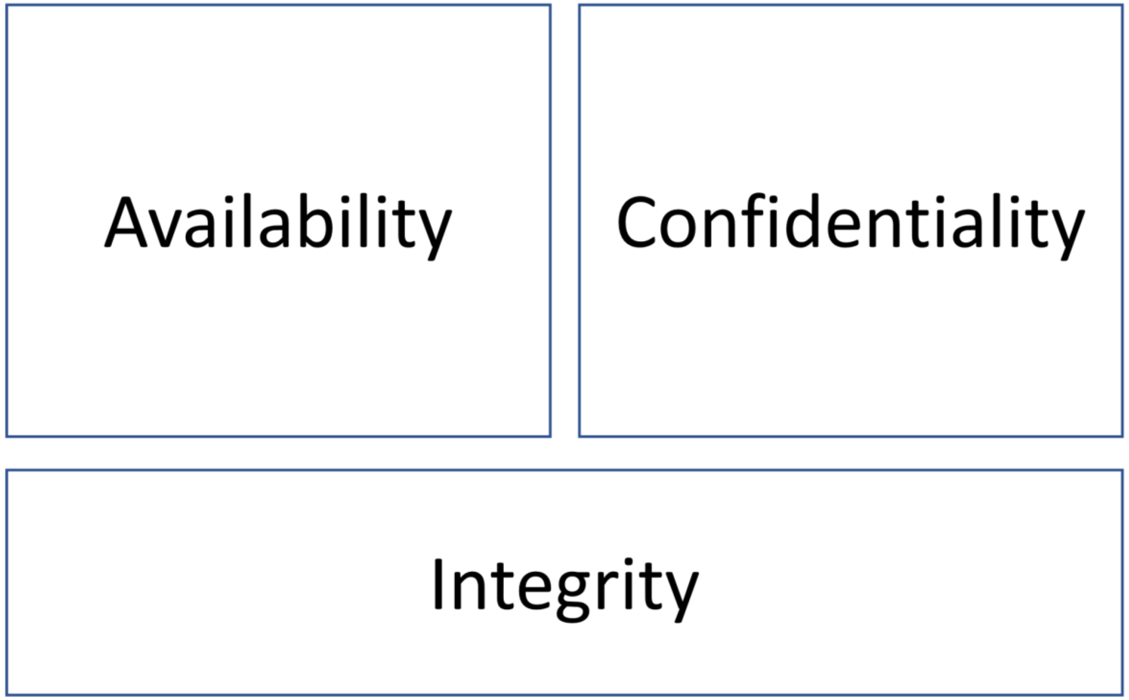
Legislation

3. A bit of history: NIS
4. Current: NIS2 Directive, Cyber Resilience Act
5. Upcoming: Cyber Solidarity Act

Takeaways

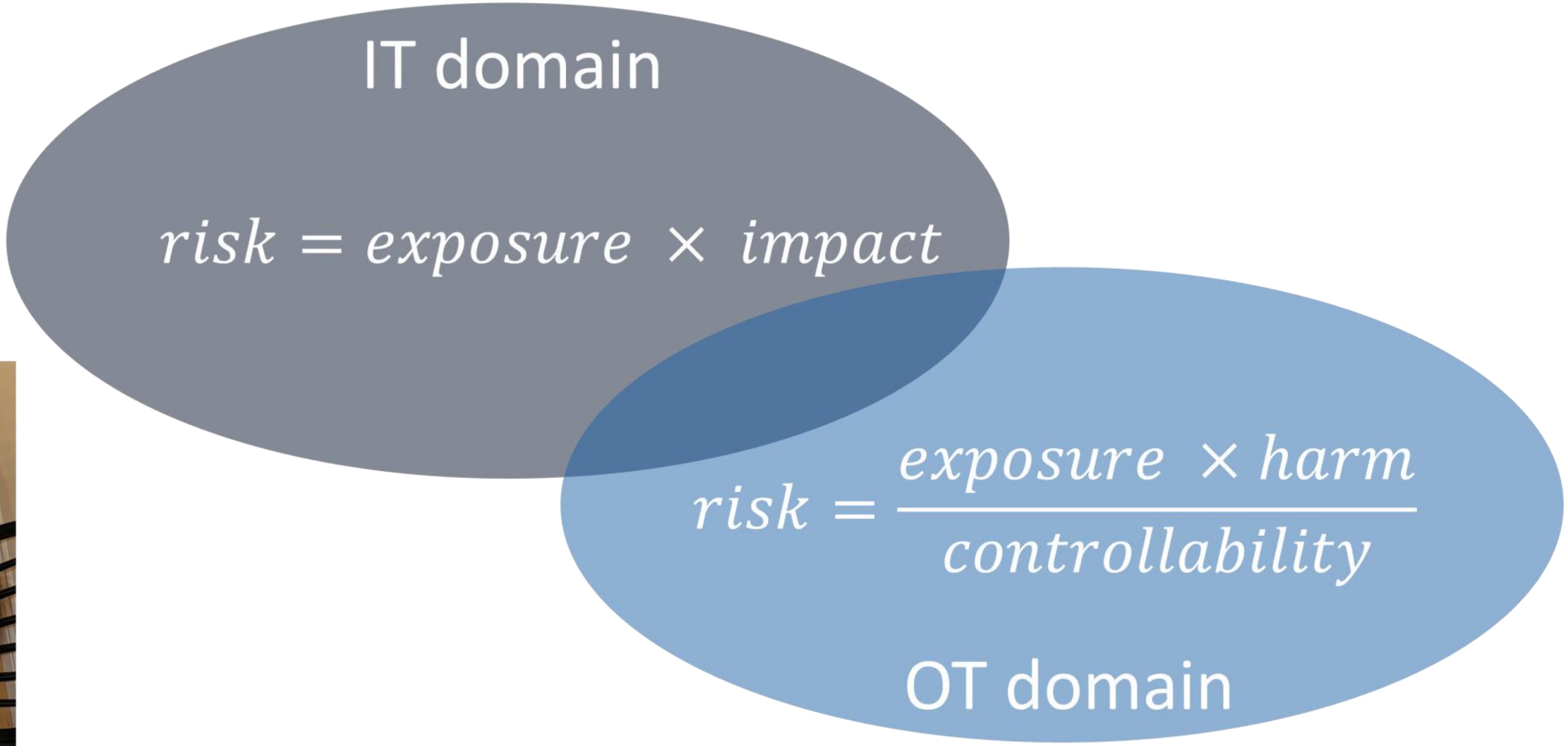
The CIA aspects

- Both availability and confidentiality can only be guaranteed (“proven”) when the system can maintain its’ own integrity.
- If you want to have your system evaluated / certified you must prove to a certain level that the system ***does*** what it must do, and ***does not*** do what it is not supposed to do.



- The new legislation adds authenticity; verification of the source.

What is risk?



IT domain

$$risk = exposure \times impact$$

$$risk = \frac{exposure \times harm}{controllability}$$

OT domain

James Conlan - Neo recently conducted his first risk assessment (2023)

Directive on the security of Network and Information Systems (2016)[1]

- Shorthand: NIS Directive
- From Cybersecurity Act: sectors regulated by NIS Directive are also sectors in which cybersecurity certification is critical.
- Entry into force 8 August 2016 / 10 May 2018

- *Authenticity*, availability, confidentiality, integrity
- Defines operators of essential services (essential for the maintenance of critical societal and/or economic activities): *energy*, *transport*, *banking*, *financial other*, *health*, *drinking water*, *digital infrastructure*

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

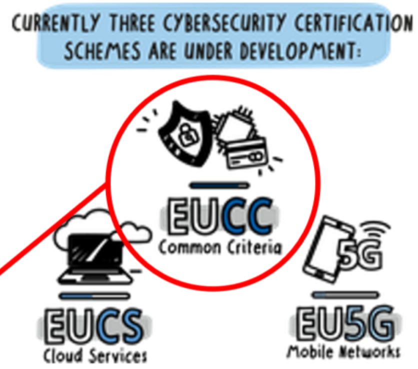
EU Cybersecurity Act (2019)[2]

- Further empowers ENISA (European Union Agency for Cybersecurity, *formerly European Network and Information Security Agency*)
- Entry into force 27 June 2019 / 28 June 2021

Security by design

Security by default

European cybersecurity certification schemes


CURRENTLY THREE CYBERSECURITY CERTIFICATION SCHEMES ARE UNDER DEVELOPMENT:
EUCC
Common Criteria
EUCS
Cloud Services
EU5G
Mobile Networks

Three assurance levels:

1. Basic
2. Substantial (attacker with limited skills & resources)
3. High (attacker with significant skills & resources)

The resulting certificate will be recognised in all EU Member States

Pictures with blue from Certification Schemes and CABs - FAQ — ENISA (europa.eu)

[2] 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)

NIS2 Directive (2022)

- More Essential & Important services (‘entities’)
- High criticality sectors (annex I)
- Other critical sectors (annex II)
- Liability for essential services
- Supply chain partners get delegated liability

Sectors of high criticality

Other critical sectors

Recent opinions

MEPs letter 12 March 2024[3]

“To be precise they could clarify that this means that organisations must start preparing for a full transition of their encryption suites as soon as possible, inter alia by:

- making an inventory of algorithms existent in their organisational infrastructure;
- reviewing the extent to which new cryptographic libraries can be used as a drop-in for current libraries in their infrastructure;
- ***ensuring that hybrid encryption, e.g. using classical as well as PQC-algorithms, is deployed where possible***; and
- start with a phased deployment as soon as NIST has adopted relevant standards.

This is especially urgent for essential and important entities in sectors of high criticality that fall under the scope of the NIS2, which will enter into force in October 2024.”

Quantum Threat Timeline Report 2023, December 2023, Global Risk Institute

“Crucially, a successful transition hinges on ***proactive technology lifecycle management***, rather than reactive crisis management, and ***will take considerable time***.”

[3] https://www.computable.nl/wp-content/uploads/2024/03/Letter-MEPs-Post-Quantum-Encryption.pdf

EU Cyber Resilience Act (2024)[4] & EU Cyber Solidarity Act (2024)

CRA

Target: wireless equipment (RED), more sectors (NIS)

Amends

- Radio Equipment Directive (2014)
- NIS directive (2016)
- Cybersecurity Act (2019)

Does not apply to equipment/products of

- Medical devices (regulation (EU) 2017/745)
- In vitro diagnostic medical devices (regulation (EU) 2017/746)
- Motor vehicles (regulation (EU) 2019/2144)
- Civil aviation (regulation (EU) 2018/1139)
- Marine equipment (directive 2014/90/EU)

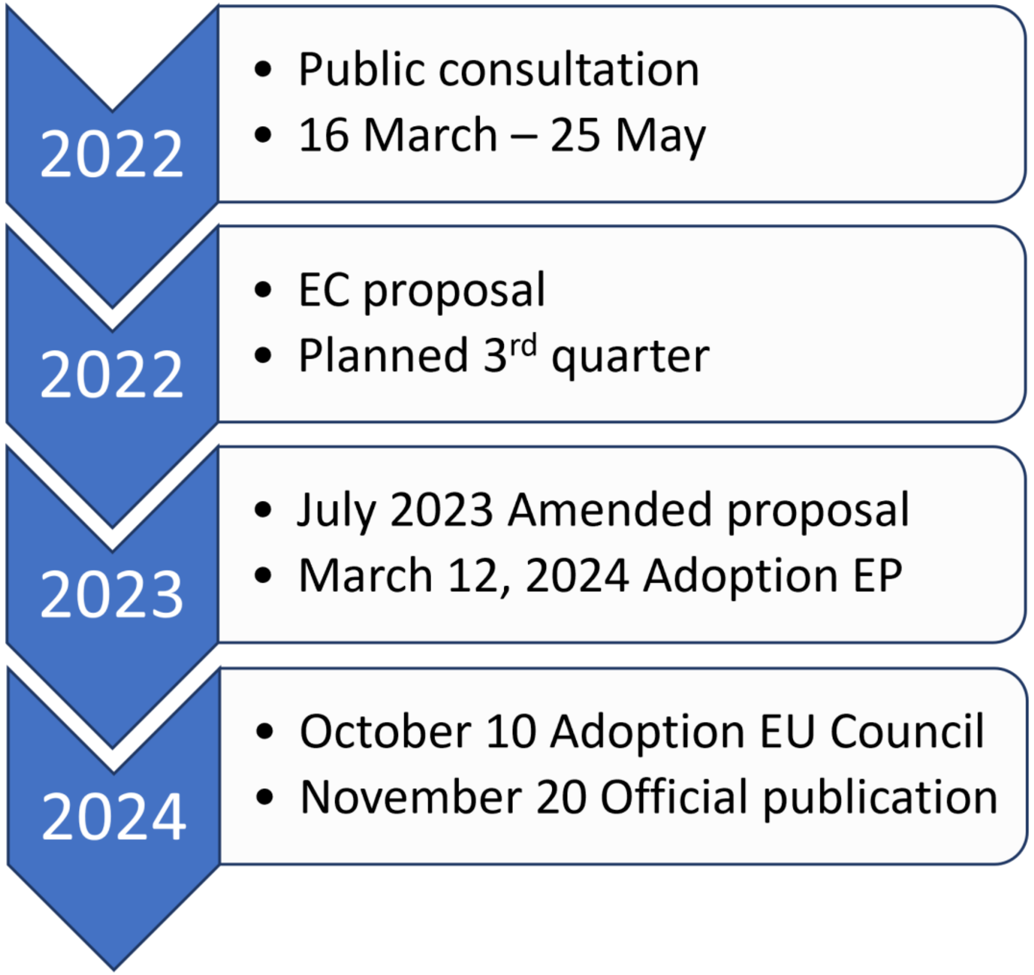
Proposal for ***regulation***

CSA 2024

Amends

- Cybersecurity Act (2019): European Cyber Shield - Security Operations Centers across EU

Proposal for ***regulation***



2022

- Public consultation
- 16 March – 25 May

2022

- EC proposal
- Planned 3rd quarter

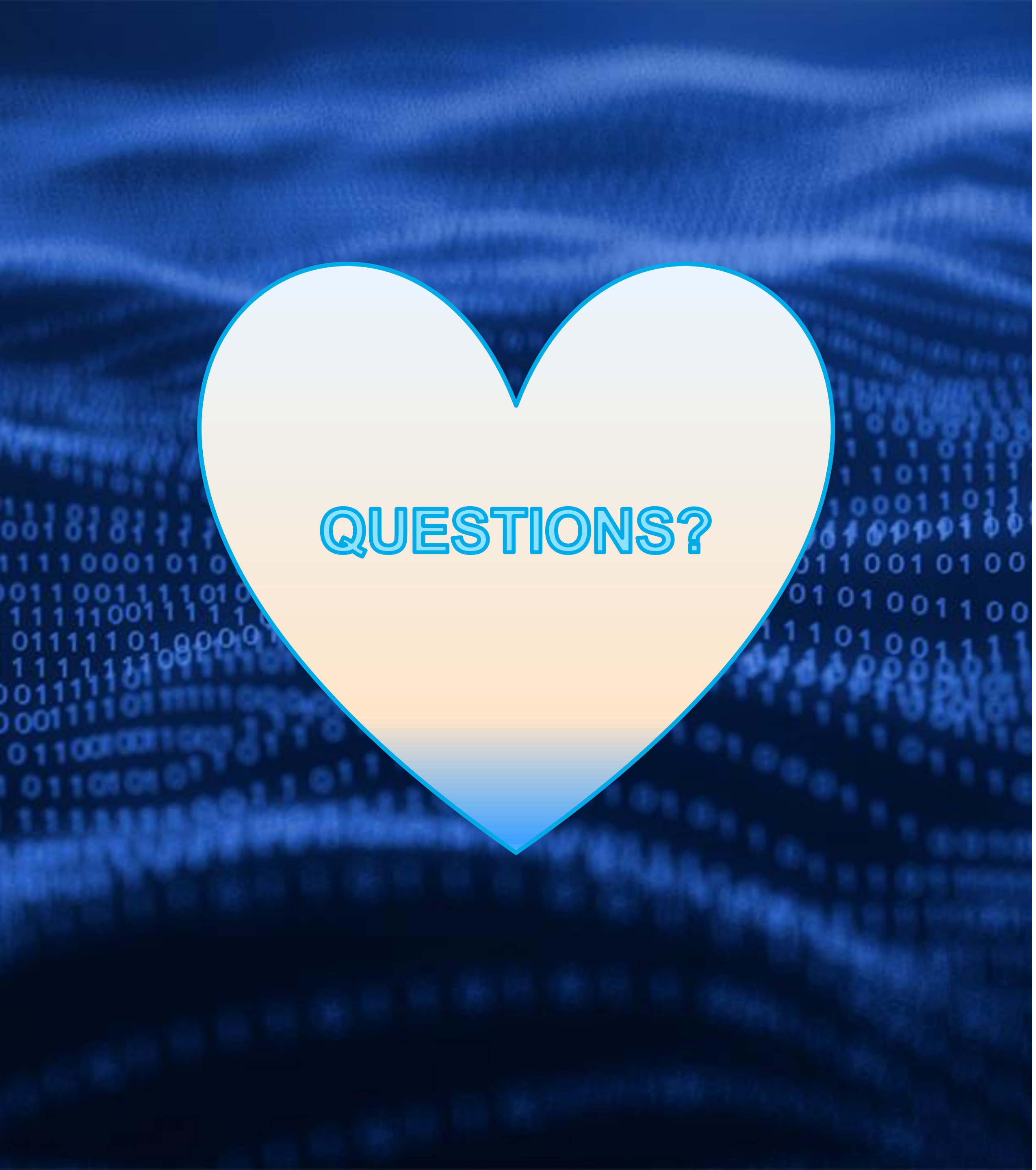
2023

- July 2023 Amended proposal
- March 12, 2024 Adoption EP

2024

- October 10 Adoption EU Council
- November 20 Official publication

[4] https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products



That’s it!

Takeaways

- General concepts (CIA, risk) are the fundament of the new legislation
- Vulnerability management essential
- Legislation covers ever more sectors, senior management explicitly accountable
- Either you’re on the commanding end (NIS2 entity) or you’re on the receiving end (NIS2 entity supplier)