Governance and Engineering

in emerging compliance frameworks

NIS2 AND CRA:
FROM LEGISLATION TO EXECUTION

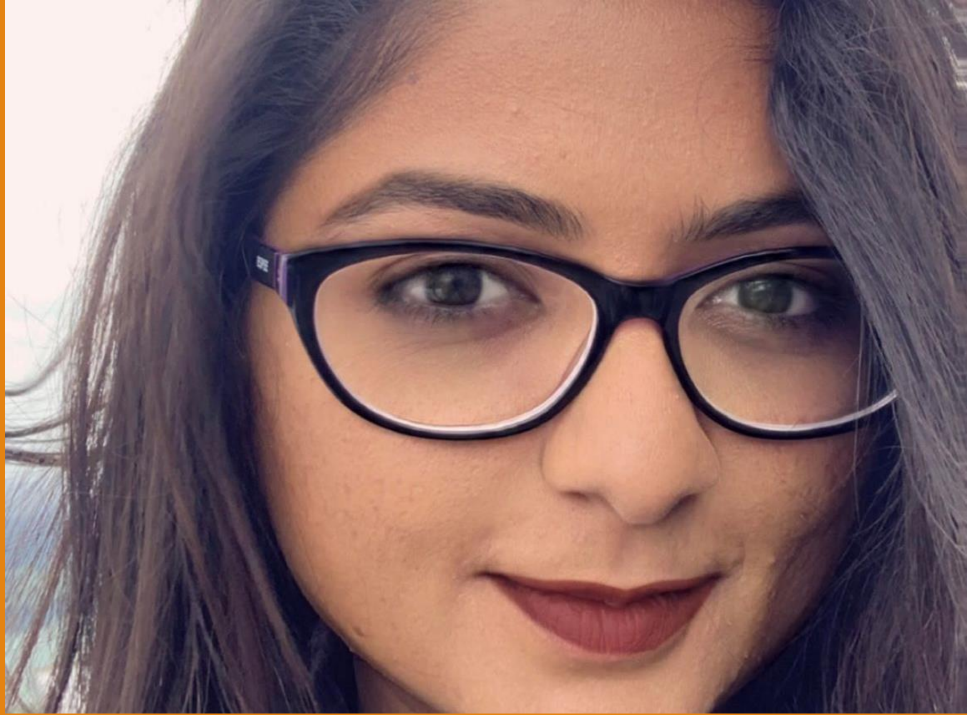
Sneha Rajguru

- Cybersecurity Enthusiast
- Star Wars superfan, and a proud LEGO builder
- When not at the desk, likely out on a long drive or testing the latest gadgets.

INTRODUCTIONS…

Jenn Janesko

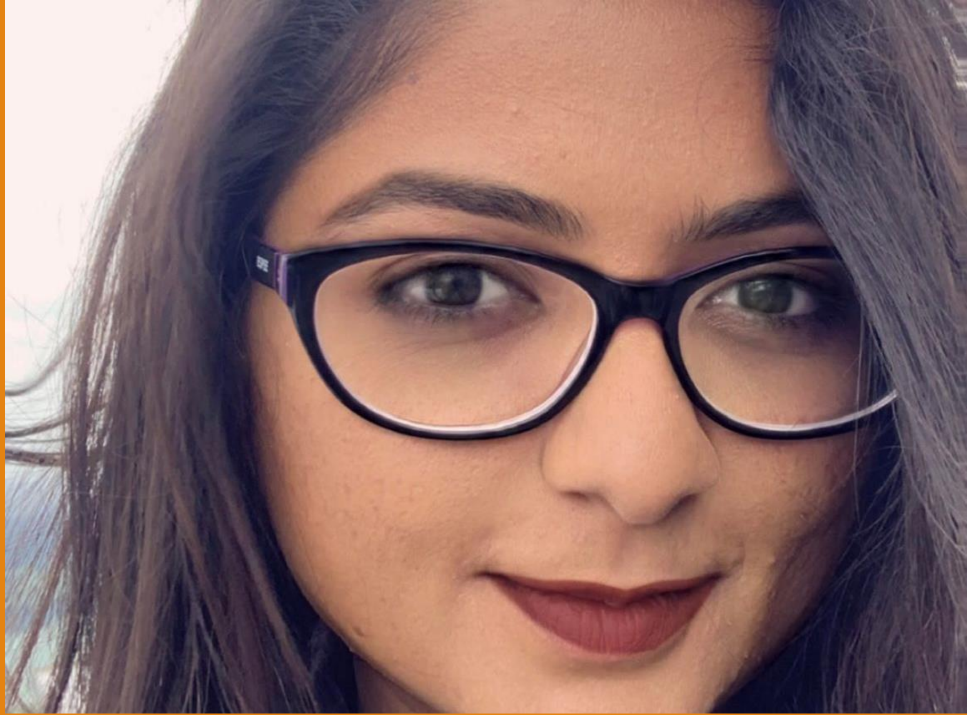
- Cyber Security and Privacy Professional
- Likes to make music, movies and 3-D models.
- When not at a desk, most likely on a mountain somewhere south of Munich.



ENGINEERING

INTRODUCTIONS...

GOVERNANCE



Roles in the Compliance Scope

Governance

1. Understand the business (structures, processes)
2. Understand external requirements placed on business
3. Identify processes, roles and responsibilities that protect the business:
    1. Satisfy the external requirements
    2. Fit the structure of the business
    3. To the extent possible:
       Reduce friction from external requirements

Engineering

1. Understand technology and best security practices
2. Help governance identify the how:
   what is possible and technically realistic
3. Help key stakeholders implement security (and provide evidence as needed)
4. Automate where possible

Network Information Systems 2 (NIS2)

and

Cyber Resilience Act

2 Emerging EU Compliance Frameworks

NETWORK INFORMATION SYSTEMS 2

Scope:

Ensure (cyber) resilience of critical infrastructure services that serve EU member states.

Timeframe:

- Adopted by Council of the European Union January 16, 2023
- EU members states required to pass corresponding laws by October 17, 2024
- Full compliance by in scope organizations, October 18, 2024

CYBER RESILIENCE ACT

Scope:

Secure products with digital elements sold in the EU throughout the product lifecycle.

Timeframe:

- Adopted by Council of the European Union October 10, 2024
- Yet to be published in the EU Official Journal
- Full compliance by in scope organizations (targeted) by November 2027

Non-Compliance: What happens?

NETWORK INFORMATION SYSTEMS 2 (NIS2)

Fines

Up to 2% of global, annual revenue or 10M€

Penalties in the case of extended non-compliance

Personal Liability

Management of entities can be held liable in cases of negligence

CYBER RESILIENCE ACT (CRA)

Fines

Up to 2.5% of global, annual revenue or 15M€

Loss of Certification

Suspension of CE certification which would result in the inability to sell products in EU market

Governance Topic

DIRECTIVE

vs.

REGULATION

1

Regulation

A piece of legislation that is passed by the Council of the European Union and must be implemented *as is* in member states.

Directive

A piece of legislation that is adopted by the Council of the European Union and member states must implement local law with the directive as a basis.

2 Emerging EU Compliance Frameworks

NETWORK INFORMATION SYSTEMS 2

NIS2

Scope:

Ensure (cyber) resilience of critical infrastructure services that serve EU member states.

Directive!

Look for detail in laws in member states.

Timeframe:

- Adopted by Council of the European Union January 16, 2023
- EU members states required to pass corresponding laws by October 17, 2024
- Full compliance by in scope organizations, October 18, 2024
- **Germany has not yet released their implementation**

NISD 2 Tracker - Bird & Bird

CYBER RESILIENCE ACT

CRA

Scope:

Secure products with digital elements sold in the EU throughout the product lifecycle.

Regulation!

Look for detail in text from EU.

Timeframe:

- Adopted by Council of the European Union October 10, 2024
- Yet to be published in the EU Official Journal
- Full compliance by in scope organizations (targeted) by November 2027

Governance: Set up processes, roles and responsibilities

Network Information Systems 2 (NIS2)

Compliance Requirements

Registration with CSIRT

Board Approval, Governance and Oversight

- Management board training awareness
- Oversight of risks
- Carry responsibility

Risk Assessment and Management

- Identify assets in scope
- Perform risk assessment
- Application security controls to manage risks
- Manage third party supplier risks
- Maintain evidence of compliance

Responsibility of Audit

- Periodic, Targeted and Ad Hoc
- Entity bears the cost of audits

Incident Response Reporting

- 24 hour report of „significant breach“
- 72 hours updated report
- 30 days – full report

Governance: Set up processes, roles and responsibilities

Cyber Resiience Act (CRA)

Compliance Requirements

Data Proteciton and Security by Default

- Perform risk assessment
- Application of security controls to manage risks
- Manage risk from third parties
- Maintain evidence of compliance

Responsibility of Conformity

- Non-important/critical products: Simplified declaration of conformity
- Important, critical products: Conformity assessment by external assessor

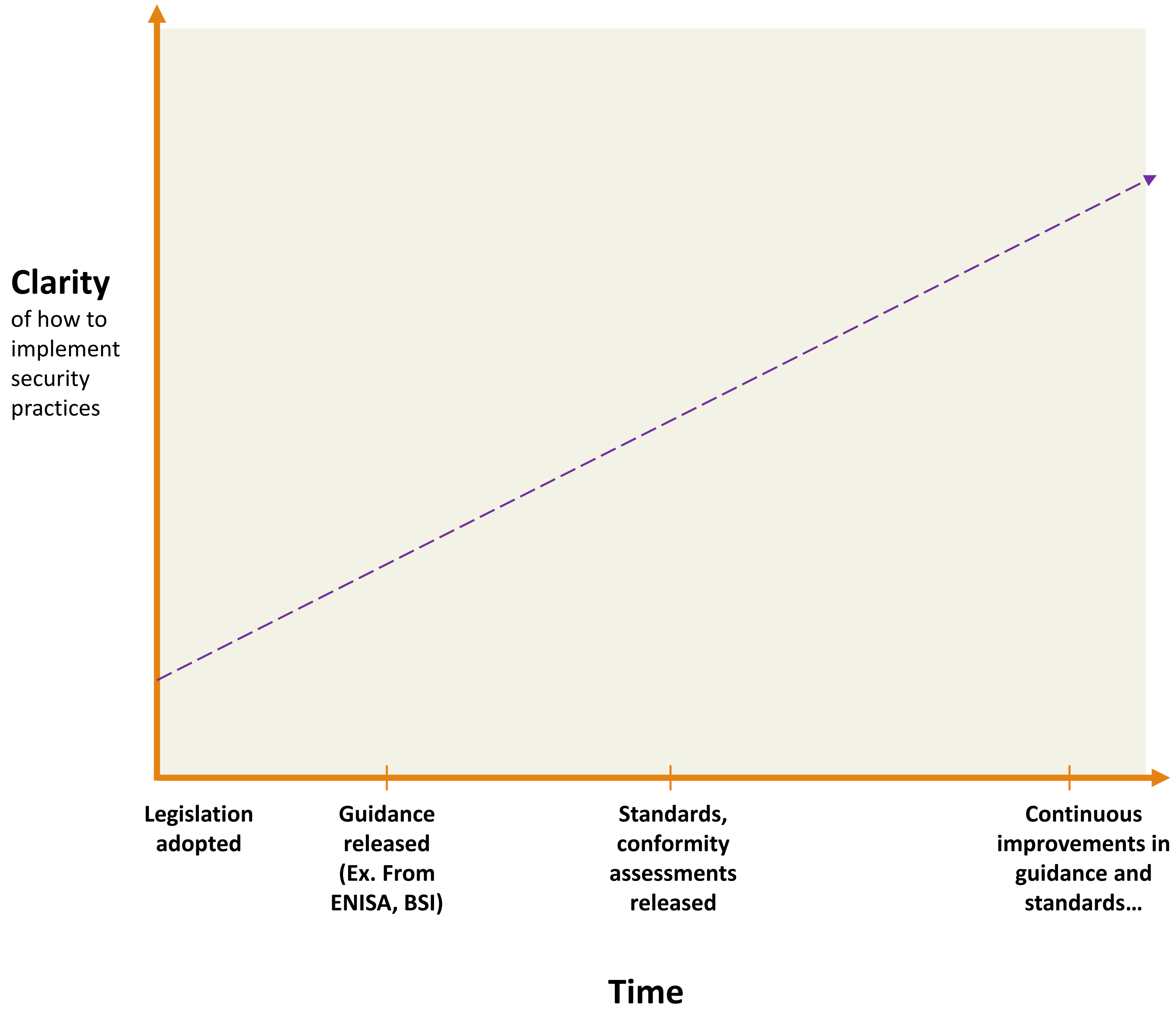
Vulnerability and Incident Response Reporting

- Coordinated vulnerability disclosure process
- Report to designated CSIRT within 24 hours of critical incident
- Provide security updates to end users for lifetime of product

Governance Engineering Handoff

In early stages of adoption, engineering and governance need to work together closely to define the „how“

Over time, more supporting material will be available to help provide more clarity of implementation



Governance - Engineering Handoff

Helpful resources…

How to implement risk assessment and security practices

CRA

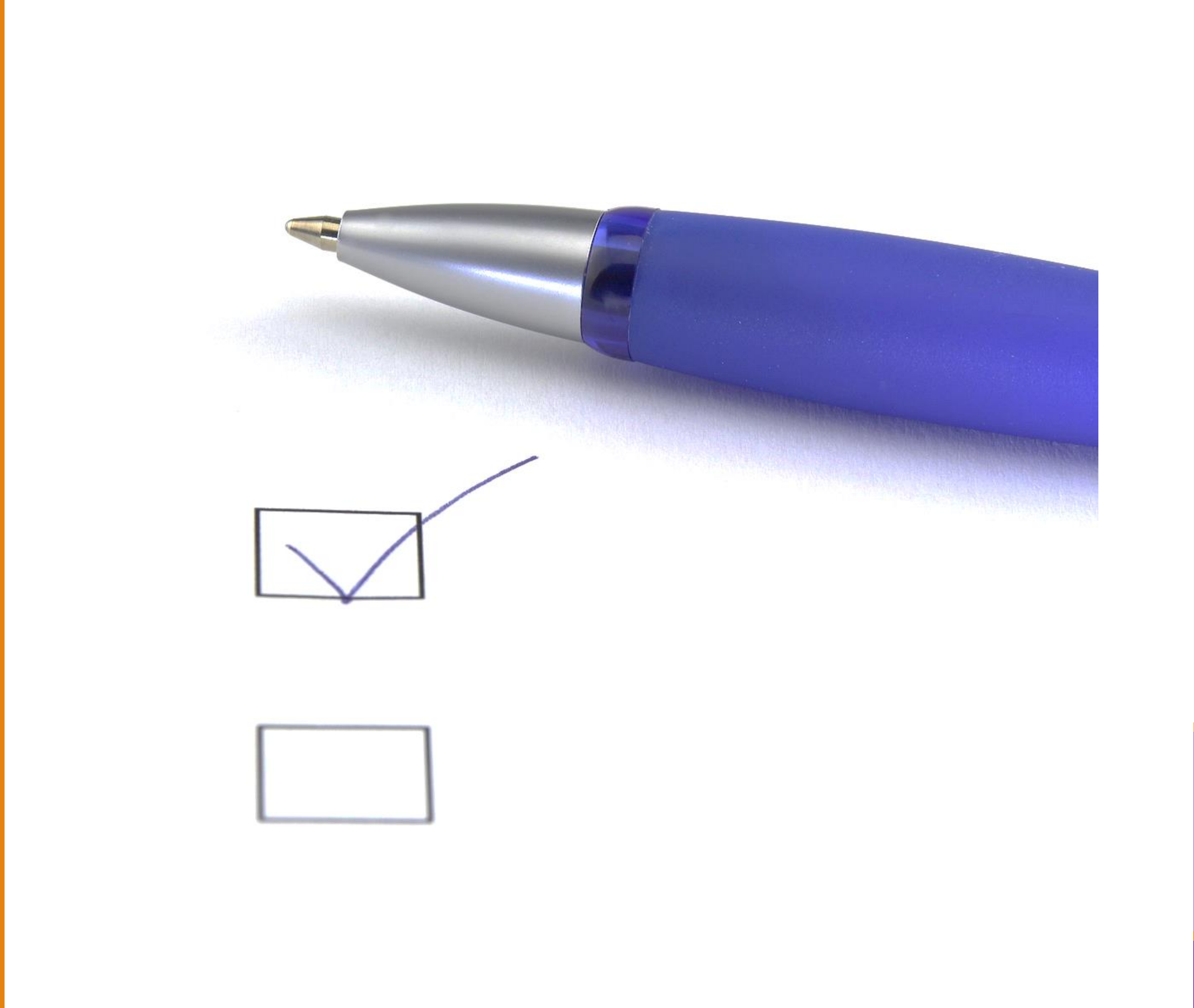
- ENISA
- BSI

NIS2

- ENISA
- BSI
- Member state guidance, laws and annexes

Governance Topic:

IS THE LEGISLATION **MATERIAL** (APPLICABLE) TO MY BUSINESS?



Materiality: Cyber Resilience Act

Secure **products with digital elements** sold in the EU throughout the product lifecycle.

Important

- *Products that present a higher cybersecurity risk by performing a function which carries a significant risk of adverse effects… to the health, security or safety of users*

Critical

- *Products have a cybersecurity-related functionality and perform a function which carries a significant risk of adverse effects…through direct manipulation.*
- *Products that are critical dependencies for essential entities referred to in Article 3(1) of Directive (EU) 2022/2555.*

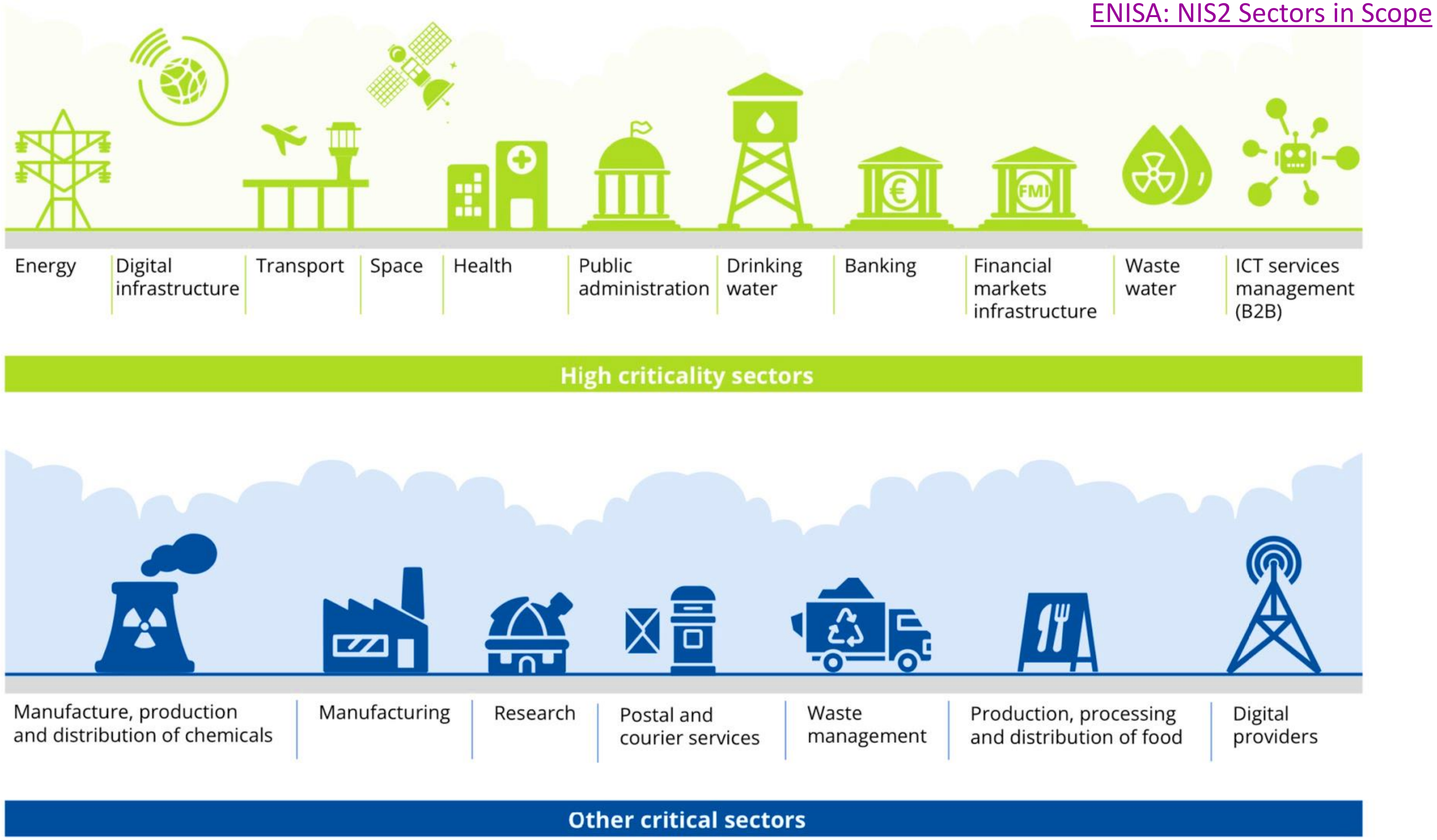
Other

- Other products with digital elements

Materiality: NIS2

Ensure (cyber) resilience of **critical infrastructure services** that serve EU member states.

ENISA: NIS2 Sectors in Scope



Is the legislation material to my business?

This is a ***legal*** question.

NIS2 and CRA are complex pieces of legislation. In both, a business must determine whether or not it is in scope. Further, it must also determine which category it falls into within the compliance framework to know which requirements are applicable.

It is important to work with legal assistance to make the decison of (level of) materiality to the business.

Recap: Roles in the Compliance Scope

Governance

1. Understand the business (structures, processes)
2. Understand external requirements placed on business
3. Identify processes, roles and responsibilities that protect the business:
    1. Satisfy the external requirements
    2. Fit the structure of the business
    3. To the extent possible:
       Reduce friction from external requirements

Engineering

1. Understand technology and best security practices
2. Help governance identify the how:
   what is possible and technically realistic
3. Help key stakeholders implement security (and provide evidence as needed)
4. Automate where possible

Questions?