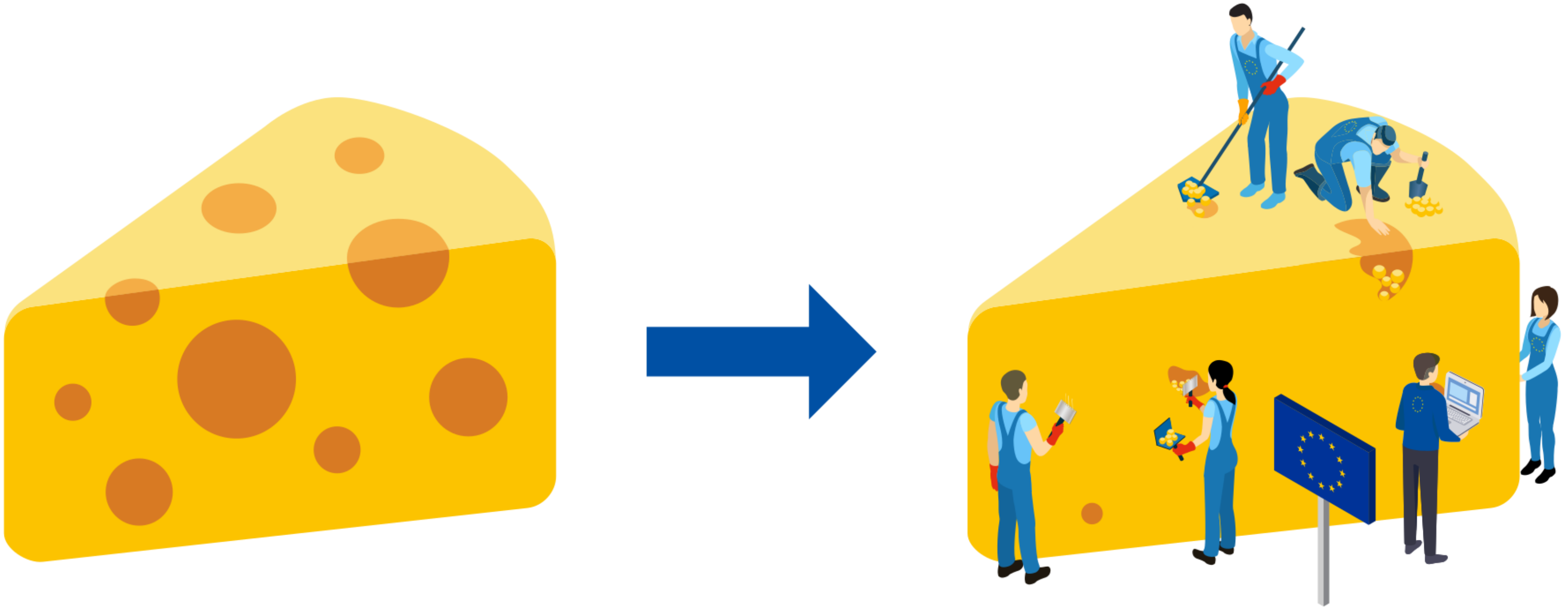
Cyber Resilience Act

Benjamin Bögel
European Commission, DG CONNECT

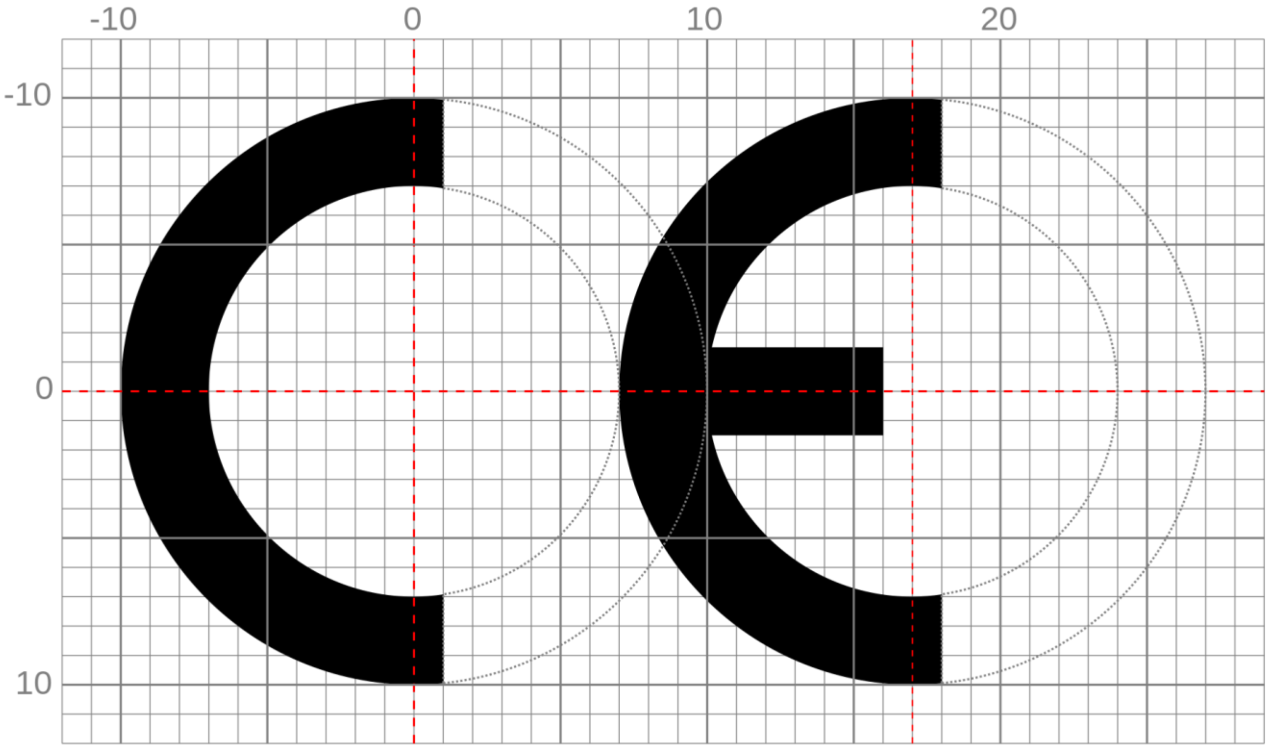
CRA in a nutshell



Main elements of the law

- **Cybersecurity rules** for the placing on the market of hardware and software
- **Obligations** for manufacturers, distributors and importers
- Cybersecurity **essential requirements** across the life cycle
- Harmonised **standards** to follow
- **Conformity assessment** – differentiated by level of risk
- **Reporting** obligations
- **Market surveillance and enforcement**

CE marking



In scope: “products with digital elements”

✓ **Hardware products** (including components placed on the market)
(laptops, smart appliances, mobile phones, network equipment or CPUs…)

✓ **Software products** (including components placed on the market)
(operating systems, word processing, games or mobile apps, software libraries…)

…including their **remote data processing solutions**!

Outside the scope

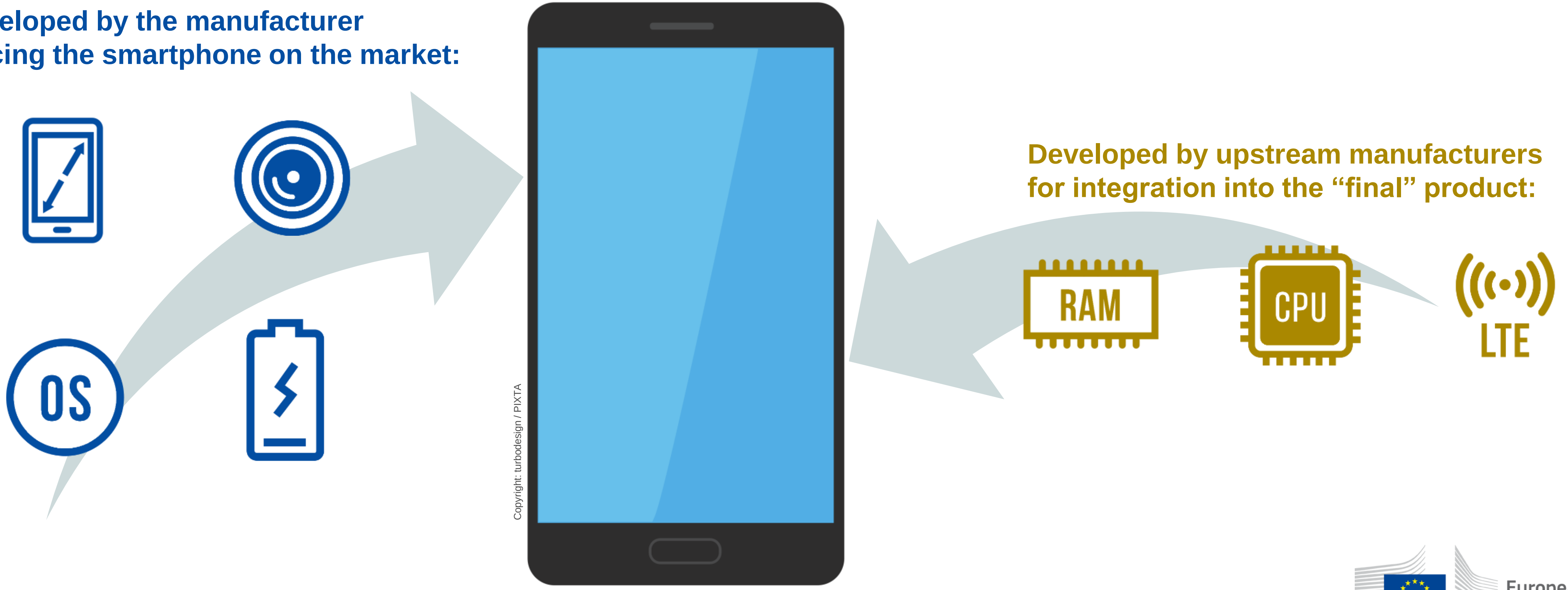
✗ **Non-commercial products**
(hobby products)

✗ **Services, in particular standalone SaaS** (covered by NIS2)
(websites, purely web-based offerings…)

✗ **Outright exclusions**
(cars, medical devices, in vitro, certified aeronautical equipment, marine equipment)

A simplified example of smartphones

As a rule, whoever places on the market a ***“final” product or a component*** *is required to comply with the* ***essential requirements****, undergo* ***conformity assessment*** *and affix the* ***CE marking.***



Developed by the manufacturer placing the smartphone on the market:

Developed by upstream manufacturers for integration into the “final” product:

Copyright: turbodesign / PIXTA

Conformity assessment – risk categorisation

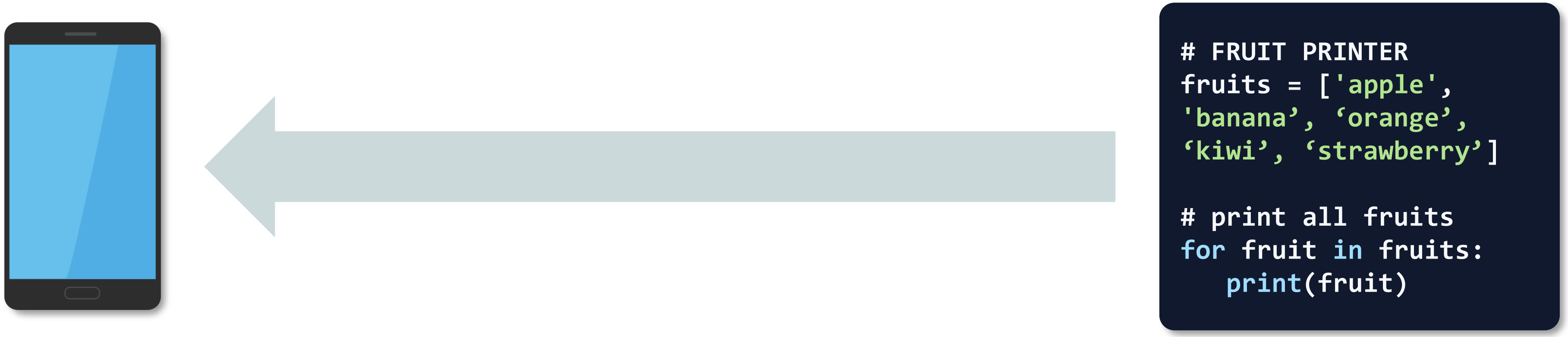
Default category — self-assessment
(memory chips, mobile apps, smart speakers, computer games...)

Important products — application of standards/third-party assessment
(operating systems, anti-virus, routers, firewalls…)

Critical products — in the future potentially certification
(smart cards, secure elements, smart meter gateways…)

FOSS — self-assessment (unless categorized as “critical products”)
(web development frameworks, operating systems, database management systems…)

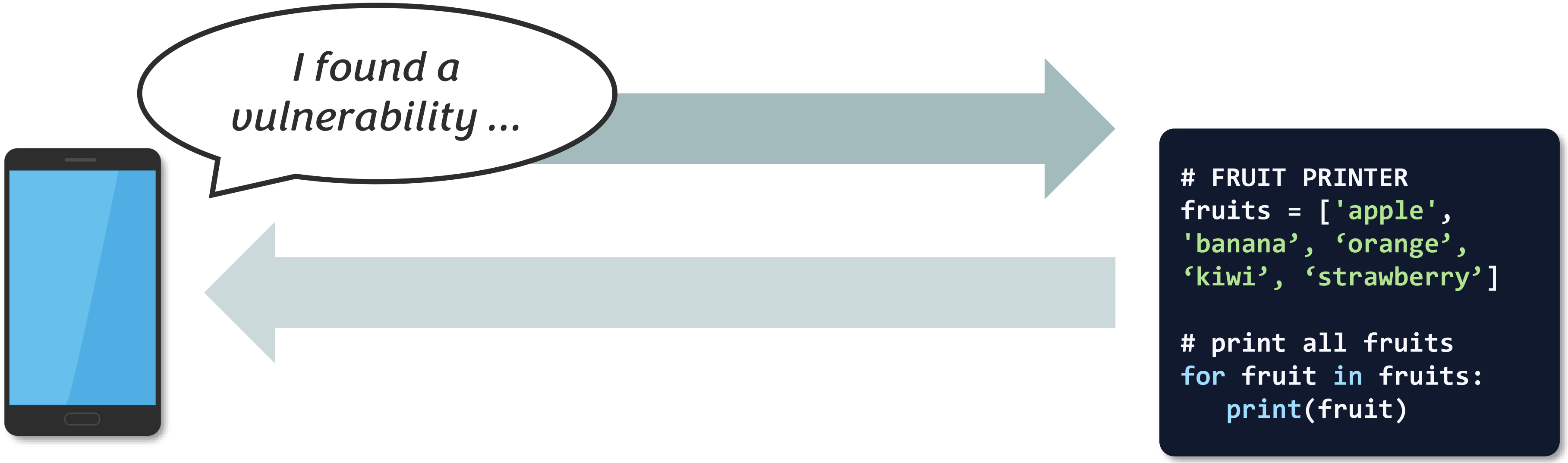
Sharing the responsibility



```
# FRUIT PRINTER
fruits = ['apple',
'banana’, ‘orange’,
‘kiwi’, ‘strawberry’]

# print all fruits
for fruit in fruits:
   print(fruit)
```

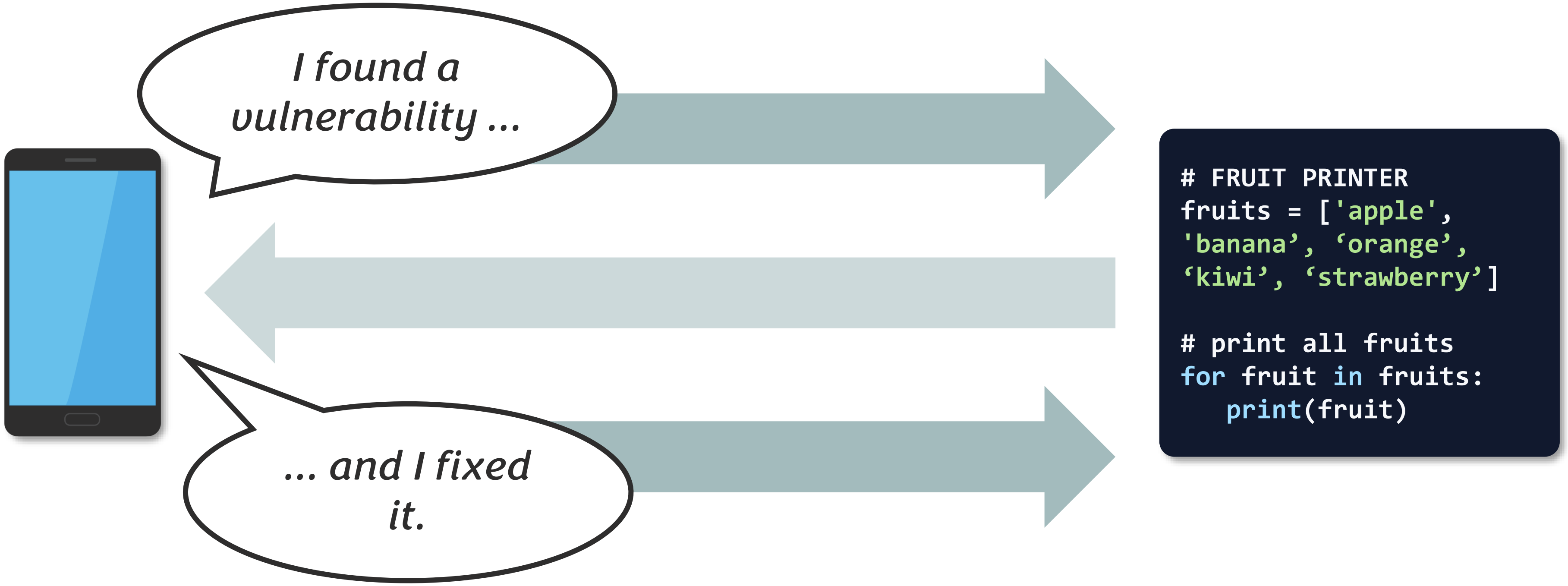
Sharing the responsibility



```
# FRUIT PRINTER
fruits = ['apple',
'banana’, ‘orange’,
‘kiwi’, ‘strawberry’]

# print all fruits
for fruit in fruits:
   print(fruit)
```

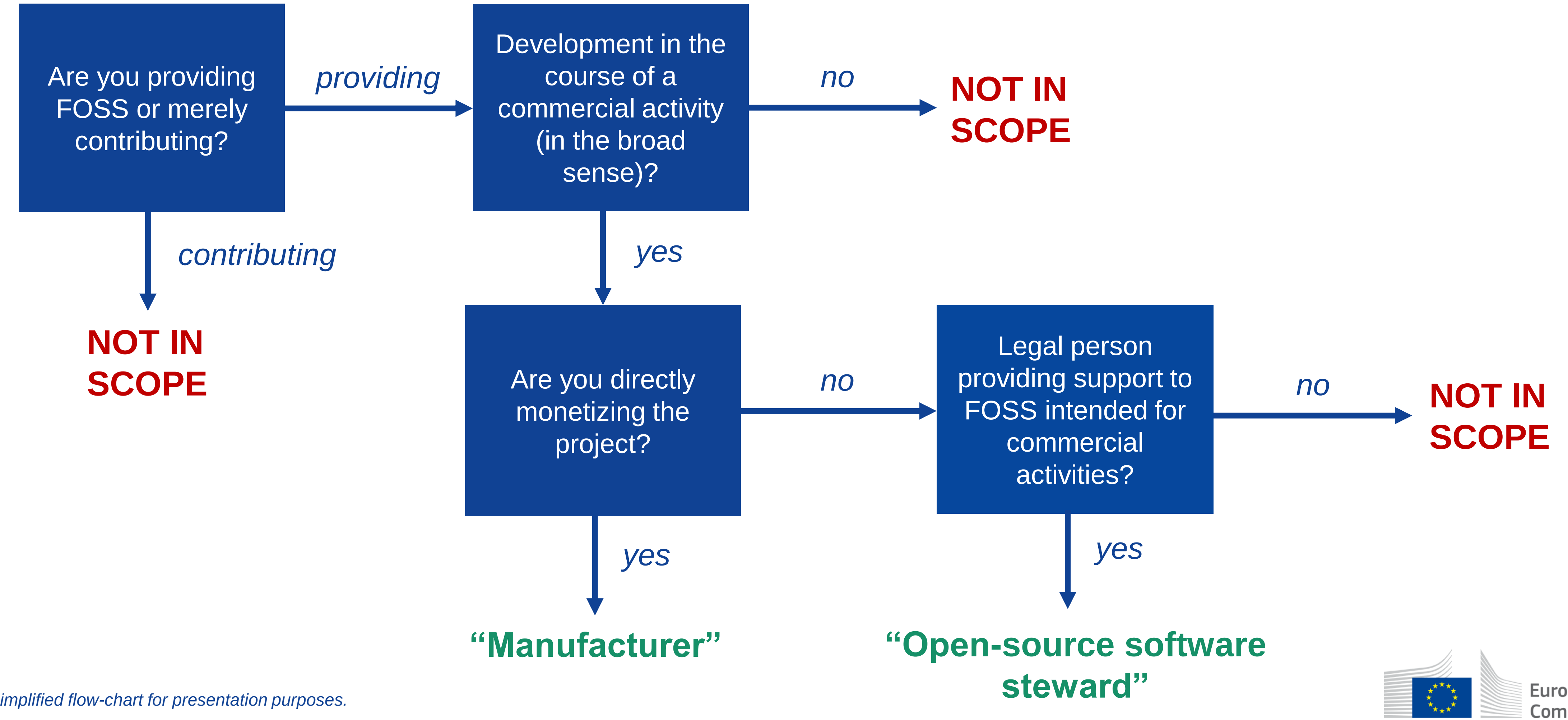
Sharing the responsibility



```
# FRUIT PRINTER
fruits = ['apple',
'banana’, ‘orange’,
‘kiwi’, ‘strawberry’]

# print all fruits
for fruit in fruits:
   print(fruit)
```

Is your open-source project covered?*



Are you providing FOSS or merely contributing?

providing

contributing

NOT IN SCOPE

Development in the course of a commercial activity (in the broad sense)?

no

NOT IN SCOPE

yes

Are you directly monetizing the project?

yes

“Manufacturer”

no

Legal person providing support to FOSS intended for commercial activities?

no

NOT IN SCOPE

yes

“Open-source software steward”

** Simplified flow-chart for presentation purposes.*

European Commission

Open-source software steward

- **Light-touch approach** for legal persons that do not directly monetise but *"support on a sustained basis the development of specific [FOSS] products [..] intended for commercial activities"*.

- **Examples:**

  - Foundations supporting specific FOSS projects
  - Companies that build FOSS for their use but make it public
  - Not-for-profit entities that develop FOSS

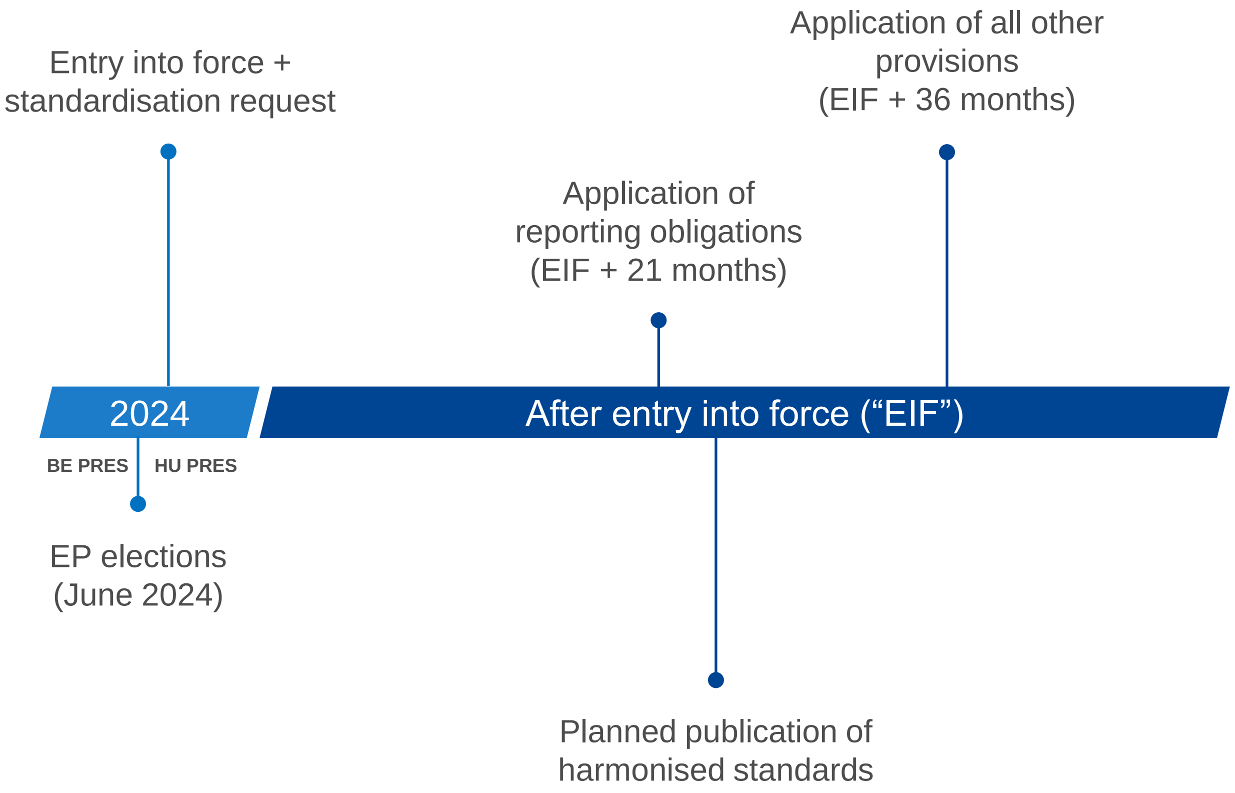
Obligations of the stewards

- Put in place a **cybersecurity policy** taking into account the specific nature of the open-source software steward

- Cooperate with **market surveillance authorities**

- **Report incidents and vulnerabilities** to the extent that they are involved in the development

Tentative timeline



Entry into force + standardisation request

Application of reporting obligations (EIF + 21 months)

Application of all other provisions (EIF + 36 months)

2024

After entry into force (“EIF”)

BE PRES

HU PRES

EP elections (June 2024)

Planned publication of harmonised standards

Thank you.

European Commission