NIS2 & Incident Management

Requirements and Assessment of Example Incidents

Laura Schöneberg, Incident Manager

18.06.26

CGI

About me

Laura Schöneberg

Incident Manager
Leinfelden-Echterdingen

NIS2 & Incident Management

01 Introduction to NIS2

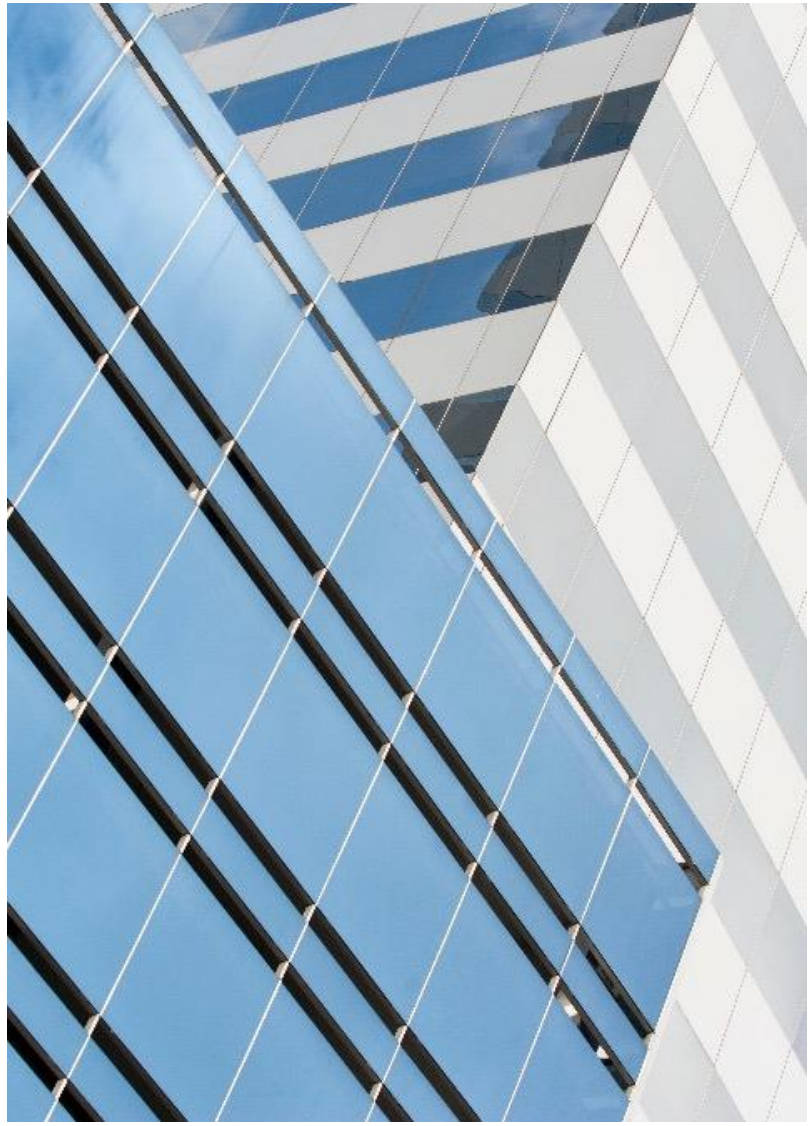
02 Requirements for Incident Management

03 Significance Criteria/Incident Assessment

04 Incident Reporting

05 Challenges & Adaptation

06 Assessment of Example Incidents



Introduction to NIS2

What is NIS2?

Legislation

- EU wide
- Cyber Security Directive
- Replaces NIS1

Scope?

Critical Sectors

- Energy, Transport, Health
- Public Administration
- Waste & Food

Public and Private Entities

Service Providers

- Managed Services
- Data Center
- Cloud Computing

Entity Classification

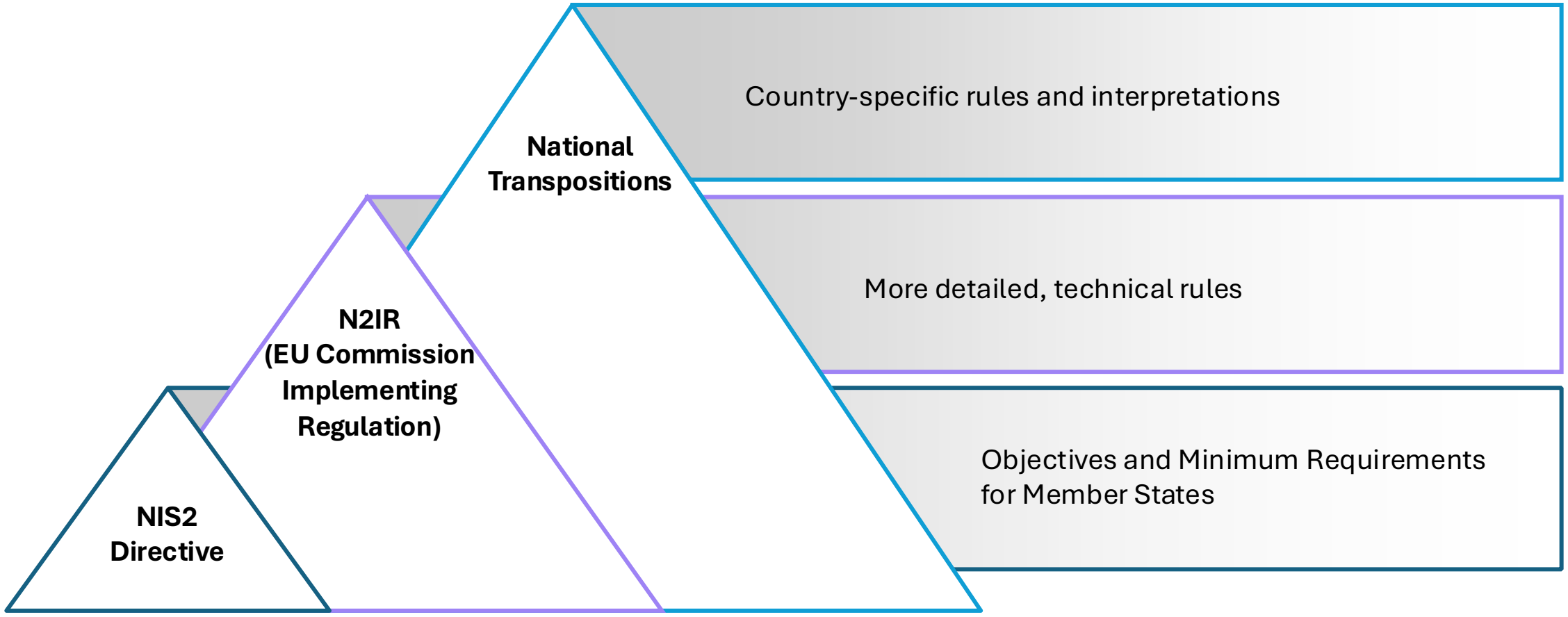
Essential Entities

- Highly critical sectors

Important Entities

- Less critical but still relevant

Directive vs National Transpositions



Key obligations under NIS2

Risk Management

- **including incident management**
- **stronger supply chain security**
- **enhanced network security**

Corporate Accountability

- **corporate management to oversee cybersecurity measures and to address cyber risks**
- **penalties for management**

Reporting Obligations

- **processes for prompt reporting of security incidents**
- **specific notification deadlines**

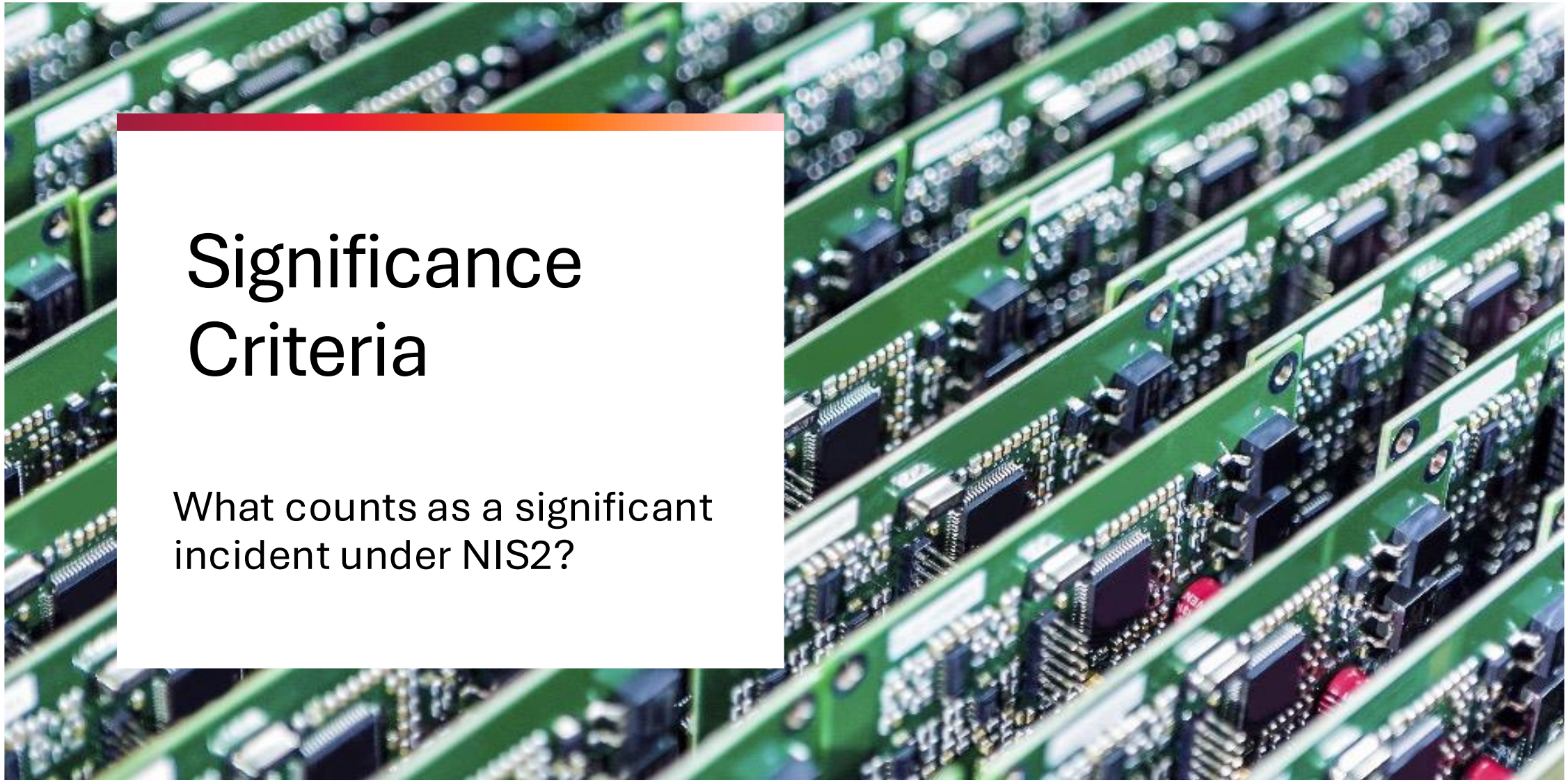
Business Continuity

- **plan for ensuring business continuity in case of major cyber incidents**
- **system recovery**
- **emergency procedures**
- **crisis response team**

What is an incident?

As defined in Article 6(6) of the NIS2 Directive:

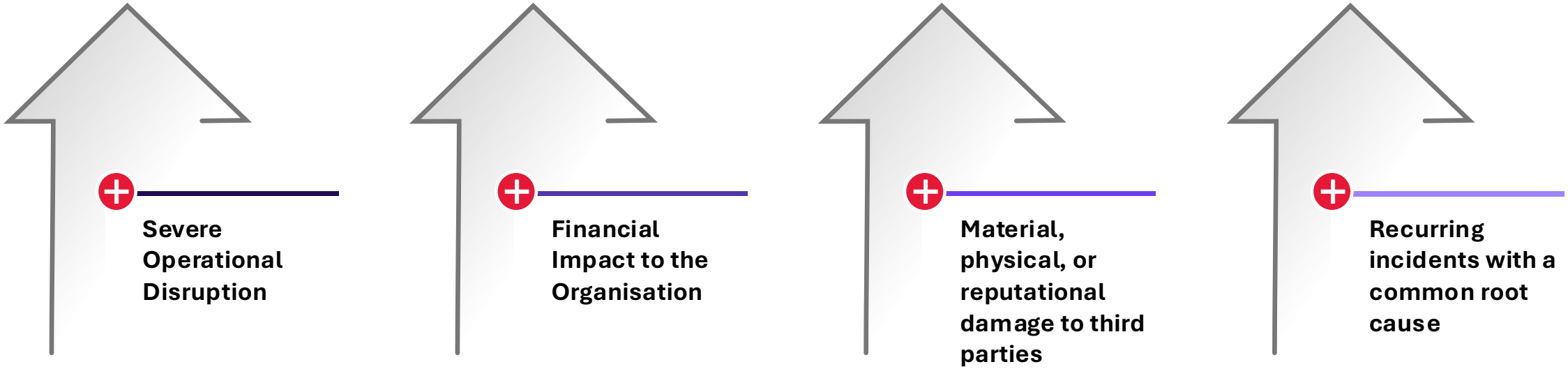
*“an event compromising the **availability**, **authenticity**, **integrity** or **confidentiality** of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems”.*



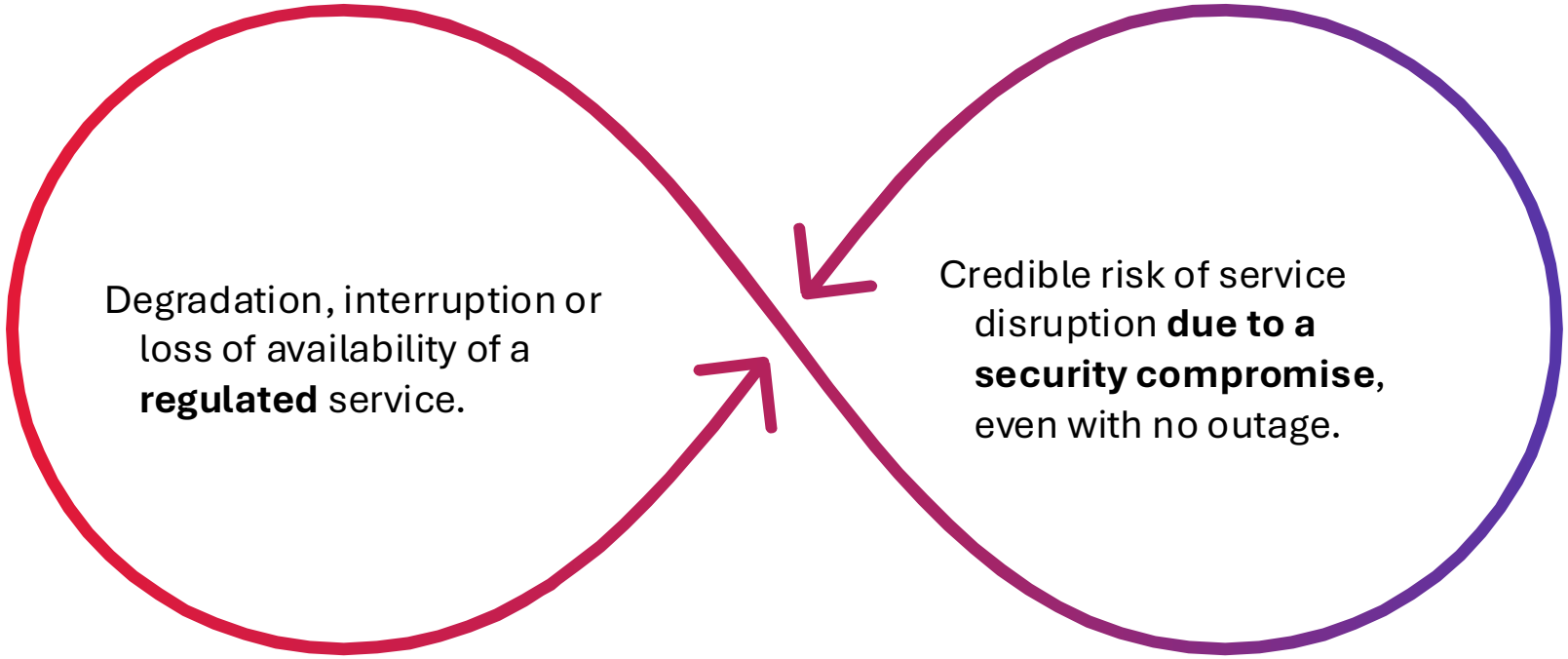
Significance Criteria

What counts as a significant incident under NIS2?

Significance Criteria



Severe Operational Disruption



"Soft failure" – The database is struggling to process queries – is it due to a security compromise?

Material, physical, or reputational damage to third parties

01

Who?

Affecting customers, partners, individuals or organizations.

02

What?

Risk of financial, physical or reputational harm.

03

How?

Damage on affected assets or serious reputational impact

Supply chain impact – can our incident cause impact to any third parties?

Recurring incidents with a common root cause

What is recurring?

two or more incidents in a **six month** timeframe

Tracking

What methods are implemented for **finding and tracking** minor incidents?

Correlation

Do you have any **automation** to support the correlation between incidents?

Common root cause?

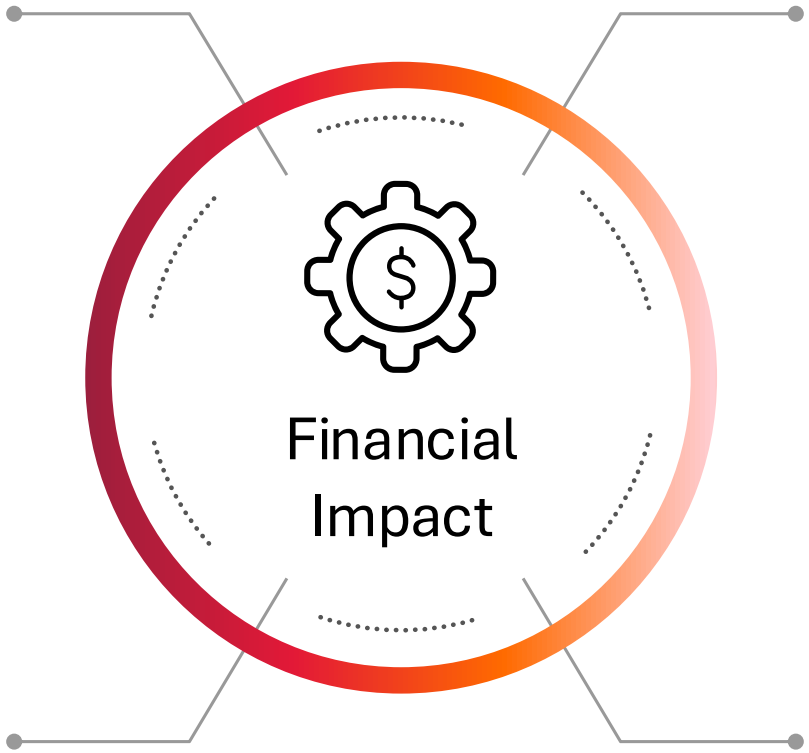
Vulnerability vs. process gap

Review

How often do you **review** your past minor incidents?

Direct financial loss exceeding **€500,000 or 5%** of the annual turnover, whichever is **lower**.

NIS2 provides **legal baseline**, no magic number.



Exfiltration of trade secrets or IP that could affect **future** revenue.

Severe operational disruption of services.

NIS2 Scope

In scope:

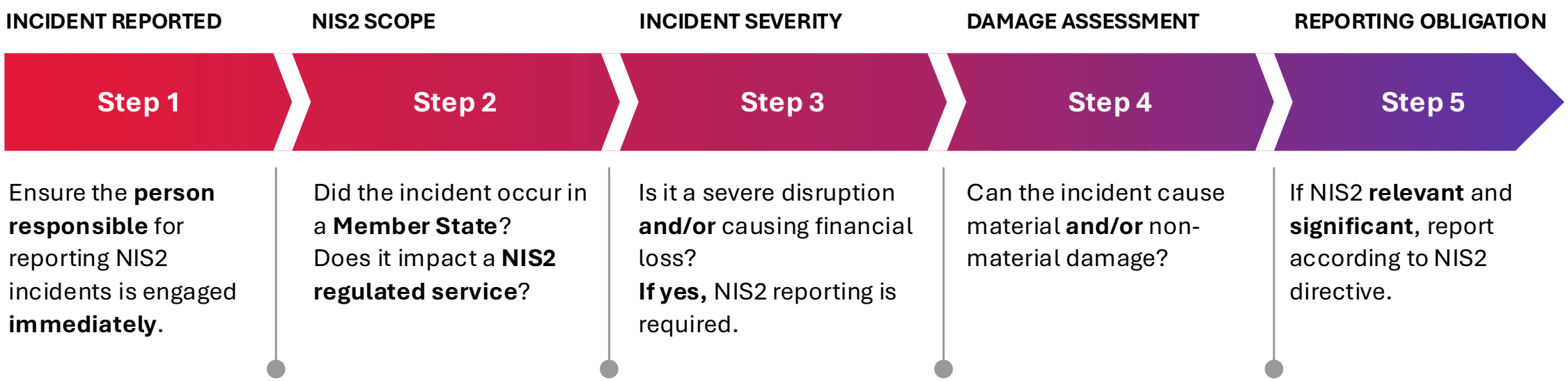
- incidents **affecting networks and information systems** that support, directly or indirectly, the provision of **NIS2-relevant services**
- Where an incident affects production systems supporting regulated services, customer-facing platforms, operational technology directly linked to service delivery, the incident must be **assessed without delay** to determine whether it qualifies as **significant**

Out of scope:

- Incidents limited to systems that are demonstrably unrelated to the provision of regulated services, and that do not create a credible risk of service disruption, financial loss, or damage to third parties, fall outside the scope of mandatory notification.

Once an incident is assessed as significant, notification is mandatory, irrespective of whether the root cause has been identified, mitigation actions are still ongoing or the full impact has been quantified.

Incident Management



Incident Reporting

What should I be reporting?
Where should this be reported?

Incident Reporting Types

Reporting categories are standardized across the EU.
Implementation details and thresholds may vary by country.

Early Warning (within 24h)	Incident Notification (within 72h)	Intermediate Report (if requested)	Final Report (within one month)
initial notification to competent authority/CSIRT	**more detailed report** (severity and impact)	**additional updates** (incident evolution)	**comprehensive analysis** (root cause and remediation)

Main Establishment

Applicability

- Essential/important entities with multi-national operations
- DNS, cloud, managed service providers
- headquartered outside the EU
- provide in-scope digital services within the EU

→ must designate a “main establishment” in one Member State

The main establishment determines the lead supervisory authority within the EU.

What is a Main Establishment?

- Central administration in the EU
- Location for key cyber security decisions

Why it matters

- determines primary supervisory authority
- cross-border supervision
- centralized governance

International vs National Incidents

Cross-Border / Global Incidents

- Reporting to Main Establishment + National Entities
- Does not replace national reporting
- Main establishment enables cross-border supervision

National Incidents

- In accordance with local regulations
- Local Assessment required
- Parallel Reporting possible
- Shared Services = Reporting to multiple national entities

Challenges & Adaptation

Which challenges are companies facing when implementing NIS2 requirements?

Severity definition ambiguity

- The definition of a “significant incident” under NIS2 is not always supported by clear quantitative thresholds.
- Organizations must make real-time decisions based on incomplete information
- Risk of inconsistent reporting (over-reporting vs. under-reporting)

Recurring incidents (common root cause)

Multiple low-impact incidents may collectively be considered **significant** if they share the **same root cause** and **occur repeatedly.**

Organizations often assess incidents **individually** and may **fail** to identify these patterns.

This can indicate underlying **systemic weaknesses** that require deeper remediation.

Tight reporting timelines (24h / 72h)

- **NIS2** requires organizations to issue an early warning within **24 hours** and a detailed notification within **72 hours.**
- These timelines begin once the organization becomes aware of the incident, **not after full investigation**.
- As a result, reporting is often required while information is still incomplete.

National implementation differences

- Although NIS2 establishes a common EU framework, each Member State implements it through national legislation.
- This leads to variations in reporting procedures, authorities, and thresholds across countries.
- For organizations operating in multiple jurisdictions, this creates additional compliance complexity.

Incident Scenarios

How do I assess an incident against NIS2 criteria?

Scenario #1: Service Disruption

Summary

ABC Consultancy provides managed infrastructure and cybersecurity services to a regional hospital group. A ransomware attack compromises the client's network via a phishing email, leading to encryption of critical systems.
ABC's SOC detects unusual activity but containment measures are insufficient to stop the attack.
Hospital operations are disrupted.

Affected Services include:

- Electronic Health Record (EHR) systems
- Laboratory Information Systems (LIS)
- Scheduling and operational planning systems (e.g., patient appointments, staff rostering, surgery scheduling)

Assessment

→ Number of affected individuals: currently unknown

→ Geographical spread: regional, France

→ Business Context: Client is a regional hospital group.

→ Duration of Service Disruption: currently six hours, still ongoing

→ Business Impact:

- ✓ > 6 hour disruption of hospital operations
- ✓ Emergency services partially diverted
- ✓ Manual processes introduced
- ✓ Patient care delays and risks

Scenario #1: Service Disruption

NIS2 Scope: Did the incident occur in a Member State or did it impact a NIS2-relevant service?

→ Yes, it occurred in France and impacted an essential service (hospital group).

Significance Criteria:

(1) Has the incident caused or is it capable of causing a severe disruption?

→ Yes. Disruption is ongoing, we don't know when the incident will be contained/remediated.

→ **NIS2 Reporting is required.**

Additionally:

- Patient Safety Risk
- ABC Consultancy is responsible as managed service/infrastructure provider

Scenario #2: Data Theft / Insider Risk

Summary

A client informs ABC Consultancy that a former ABC consultant may have exfiltrated sensitive client data prior to leaving the company. During the investigation, ABC Consultancy identifies evidence of data exfiltration involving both client and internal ABC data. It is further discovered that the former employee has joined a direct competitor of the client.

Affected Data includes:

- Internal ABC Consultancy documents
- Engineering and design documentation (sensitive defense-related information)
- Confidential client project data

Assessment

→ Geographical spread: Germany

→ Business Context: Client is a supplier of automotive and defense-related technologies.

→ Business Impact:

- ✓ Potential exposure of sensitive defense-related information
- ✓ Potential Financial Impact, competitive disadvantage
- ✓ Reputational Impact and loss of client trust
- ✓ Supply-chain relevance

Scenario #2: Data Theft / Insider Risk

NIS2 Scope: Did the incident occur in a Member State or did it impact a NIS2 relevant service?

→ Yes, it occurred in Germany and impacted a NIS2-relevant service (defense)

Significance Criteria:

(1) Has the incident caused or is it capable of causing a **severe disruption**?

→ No signs of that.

(2) Has the incident caused or is it capable of causing a significant **financial loss**?

→ Yes, it could cause a potential financial loss.

(3) Has the incident caused or is it capable of causing **material** or **non-material/reputational damage**?

→ Yes, reputational damage as well as competitive disadvantage is possible.

→ **NIS2 Reporting is required.**

Scenario #3: Leakage of Data

Summary

An end customer identifies a potential data exposure affecting a cloud-based customer portal managed by ABC Consultancy. Following a recent application update introduced approximately three weeks earlier, limited customer account information became unintentionally accessible online. The exact root cause remains under investigation. No operational business impact has been identified.

Affected Services include:

- customer support application

Affected Data includes:

- end customer account details
- internal support ticket references
- limited business contact information

Assessment

→ Number of affected users: ~80 end customers

→ Geographical spread: Finland

→ Business Context: Logistics Provider

→ Root cause is still being investigated

Scenario #3: Leakage of Data

NIS2 Scope: Did the incident occur in a Member State or did it impact a NIS2 relevant service?

→ Yes, it occurred in Finland.

Significance Criteria:

(1) Has the incident caused or is it capable of causing a **severe disruption**?

→ No signs of that.

(2) Has the incident caused or is it capable of causing a significant **financial loss**?

→ No signs of that.

(3) Has the incident caused or is it capable of causing **material** or **non-material/reputational damage**?

→ No signs of that.

→ At the moment, NIS2 Reporting might not be required.

→ Incident should be reassessed as it progresses.

Recap

- ✓ NIS2 Scope
- ✓ Directive vs National Transpositions
- ✓ Definition Security Incident
- ✓ Significance Criteria
- ✓ Incident Assessment
- ✓ Reporting Obligations
- ✓ Main Establishments
- ✓ Cross-Border Incidents
- ✓ Challenges & Adaptation
- ✓ Assessment of Example Incidents

Questions?