

WHAT YOU NEED TO KNOW



The NIS2 directive is a flagship EU-wide legislation on cybersecurity.

Its aim is to ensure a high common level of cybersecurity across the Union on the basis of three pillars:

NIS2 requires **each Member State** to transpose its provisions into national law by 17 October 2024

NATIONAL CAPABILITIES

- Cybersecurity strategy
- National Competent Authority (NCA)
- Cybersecurity Incident Response Team (CSIRT)
- Coordinated vulnerability disclosure policy
- Cyber crisis management framework

COOPERATION AT UNION LEVEL

- NIS Cooperation Group
- CSIRTs Network
- EU-CyCLONe
- EU vulnerability database
- EU registry for entities
- Report on the state of the Union on cybersecurity

OBLIGATIONS FOR ENTITIES

- Cybersecurity risk management measures
- Incident reporting
- Responsibility of management bodies

MEMBER STATE RESPONSIBILITIES

Drafting National Legislation



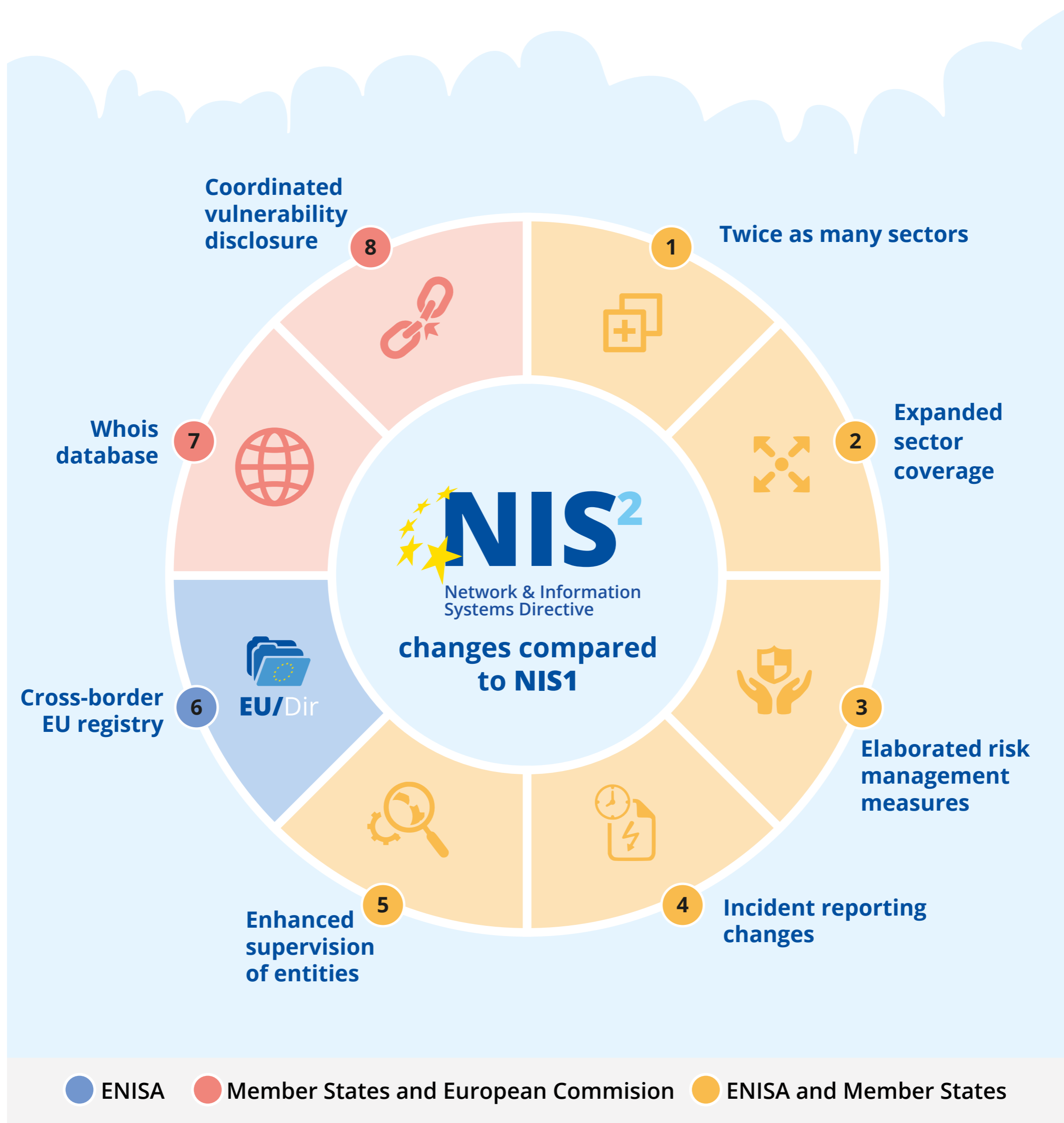
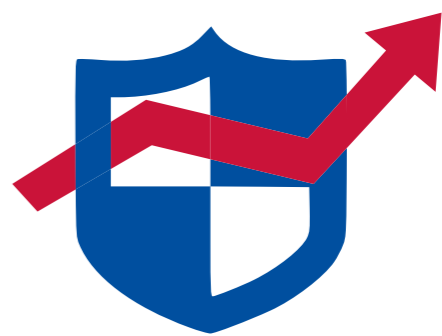
Setting Implementation Timelines











Enforcement and Oversight via designated National Authorities



FROM NIS1 TO NIS2: WHAT'S NEW



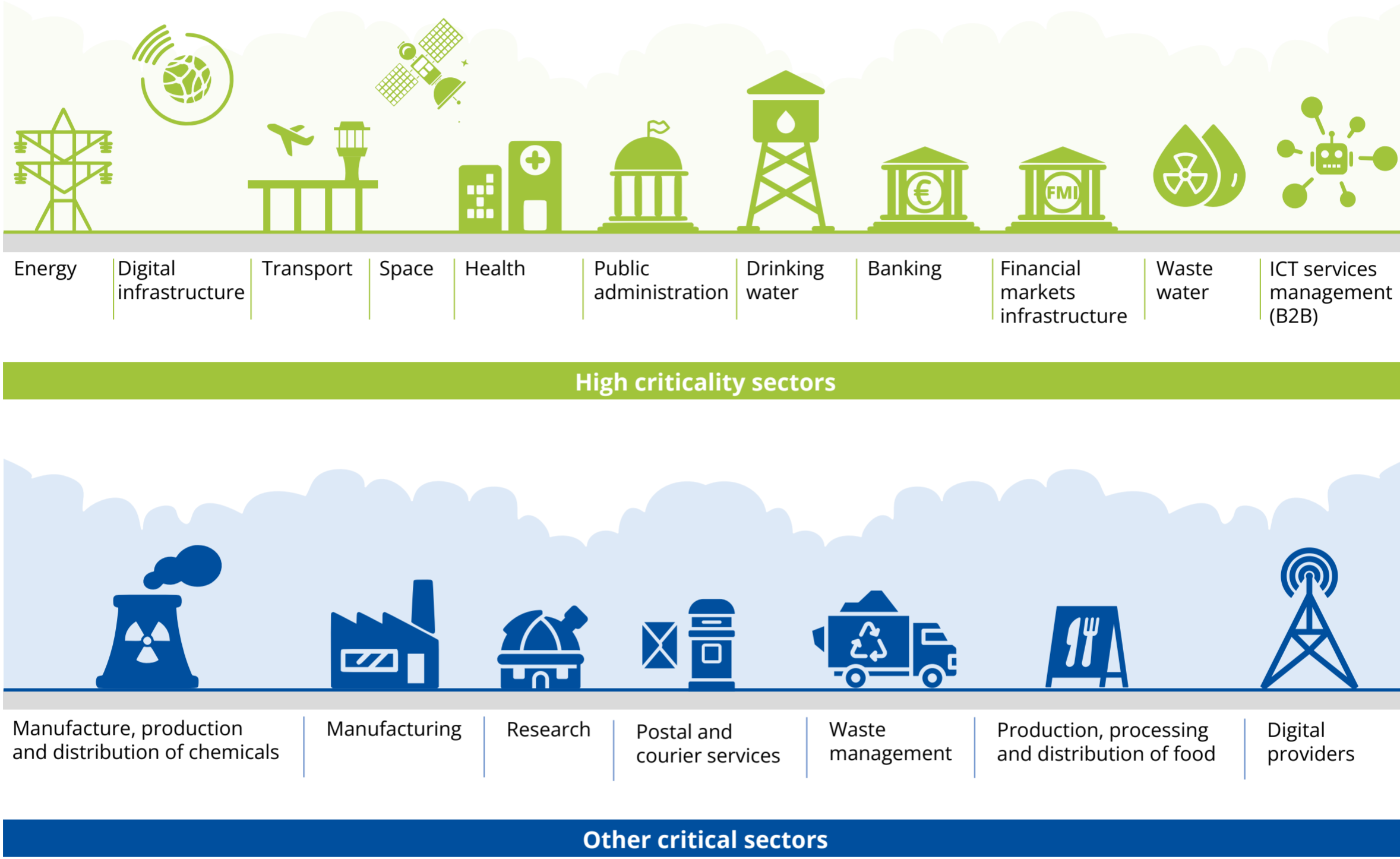
<div>■ 1 Twice as many sectors</div> <div></div> <div>With NIS2 more sectors / subsectors are in scope based on their degree of digitalization, interconnectedness and how crucial they are for the economy and society.</div>	<div>■ 2 Expanded sector coverage</div> <div></div> <div>A size threshold rule distinguishes essential from important entities, while Member States can include smaller, high-risk entities.</div>	<div>■ 3 Elaborated risk management measures</div> <div></div> <div>An expanded list of proportional, all-hazards cybersecurity risk management measures is introduced, along with increased responsibilities for top management.</div>
<div>■ 4 Incident reporting changes</div> <div></div> <div>More structured incident notification obligations apply to in-scope organisations, with specific deadlines for incidents which have a 'significant impact' on the provision of their services.</div>	<div>■ 5 Supervision of entities</div> <div></div> <div>A more coherent framework for stronger supervision is introduced, that encompasses minimum supervisory means, distinct regimes for essential and important entities, and cross-border collaboration mechanisms.</div>	<div>■ 6 Cross-border EU Registry</div> <div> EU/Dir</div> <div>An EU-wide registry for cross-border entities where Member States will register their main establishments and branches is foreseen for enhanced supervision.</div>
<div>■ 7 Whois database</div> <div></div> <div>Member States are expected to maintain a dedicated database of domain name registration data, including contact details for registrants and administrators, to enhance DNS security, stability, and resilience.</div>	<div>■ 8 Coordinated vulnerability disclosure</div> <div></div> <div>A structured process for reporting vulnerabilities to manufacturers or service providers, is introduced, to ensure vulnerabilities are addressed and resolved before being made public.</div>	

SECTORS IN SCOPE



The NIS2 directive identifies several sectors that are considered crucial for the functioning of the economy and society.

These sectors are classified into two main categories: **sectors of high criticality** & **other critical sectors** and include:



Entities within the identified sectors are categorized as **essential entities** or **important entities**

depending on factors such as size, sector and criticality.

Essential entities	Important entities
<ul style="list-style-type: none">• High criticality sectors - companies that exceed mediumsized threshold• Qualified trust service providers and top- level domain name registries, regardless of size• DNS service providers, regardless of size• Providers of ECN or ECS - medium-sized and large companies	<ul style="list-style-type: none">• High criticality sectors - companies that are small or medium• Other critical sectors - companies that exceed medium- sized threshold• Providers of ECN or ECS - small companies

KEEP IN MIND

<div>■ 1</div> <div>All entities are required to implement risk management measures.</div> <div></div>	<div>■ 2</div> <div>All entities are required to report significant cybersecurity incidents.</div> <div></div>	<div>■ 3</div> <div>Essential entities are subject to ex ante & ex post supervision.</div> <div></div>	<div>■ 4</div> <div>Important entities are subject to ex post supervision only.</div> <div></div>
--	--	--	---

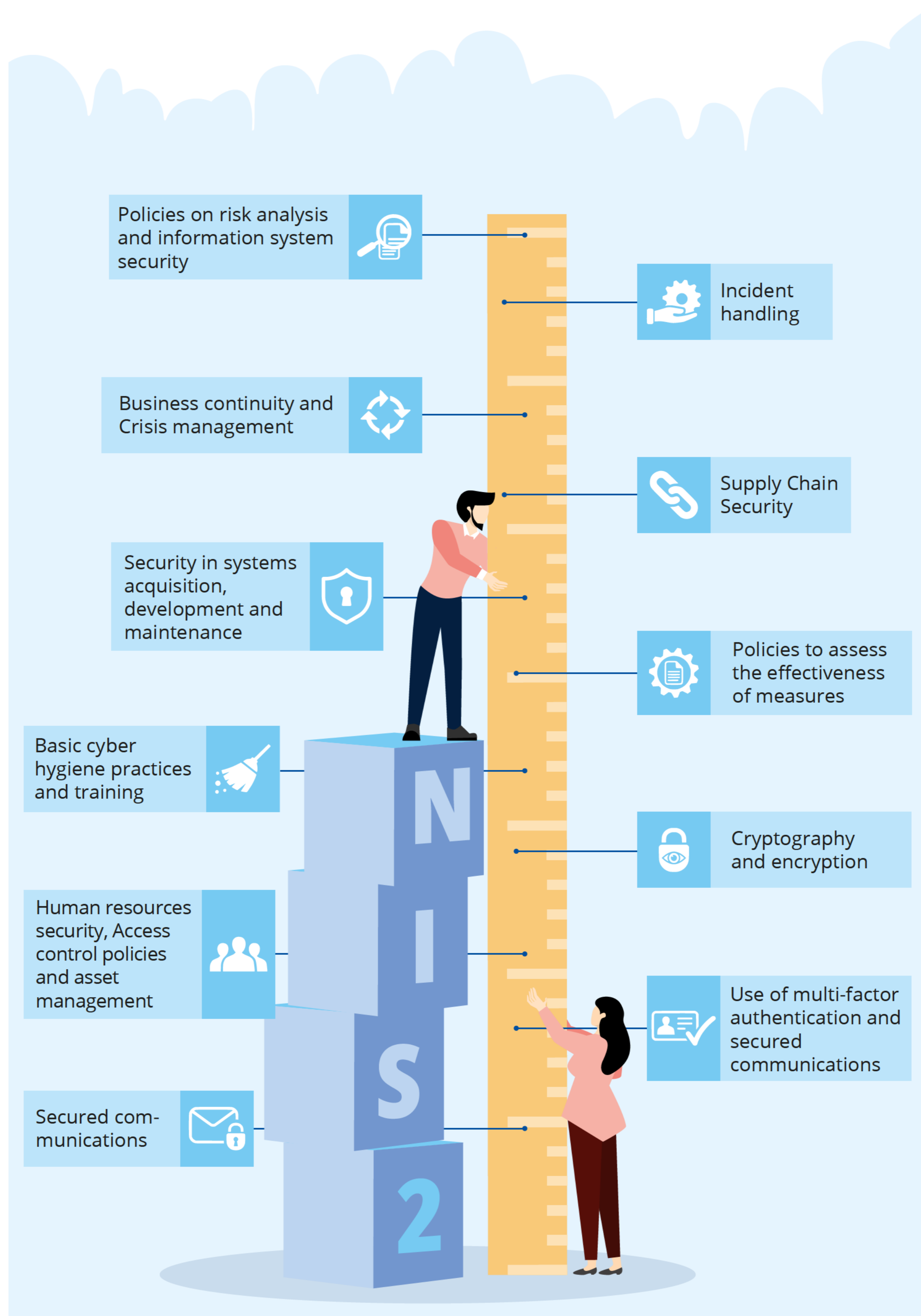


CYBERSECURITY RISK MANAGEMENT MEASURES



Organisations are required to implement technical, operational, and organizational measures to effectively manage risks to their systems and

minimize the impact of incidents. These must be based on an all-hazards approach and include at minimum the following:



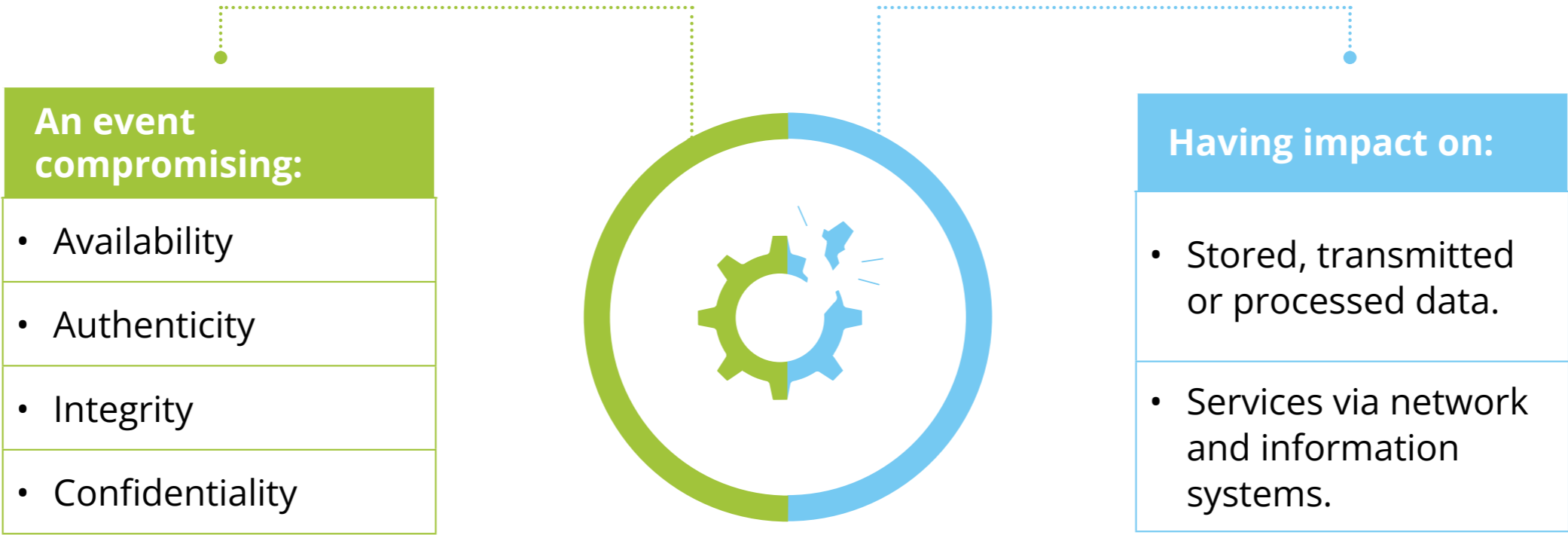
INCIDENT REPORTING



Effective and timely reporting of significant incidents is a cornerstone of the NIS2 directive. It enables a deeper understanding of their impact, improves response capabilities and advances cyber resilience.



■ WHAT IS AN INCIDENT?



■ WHEN SHOULD I REPORT?

When becoming aware of a **significant incident**:



■ 1

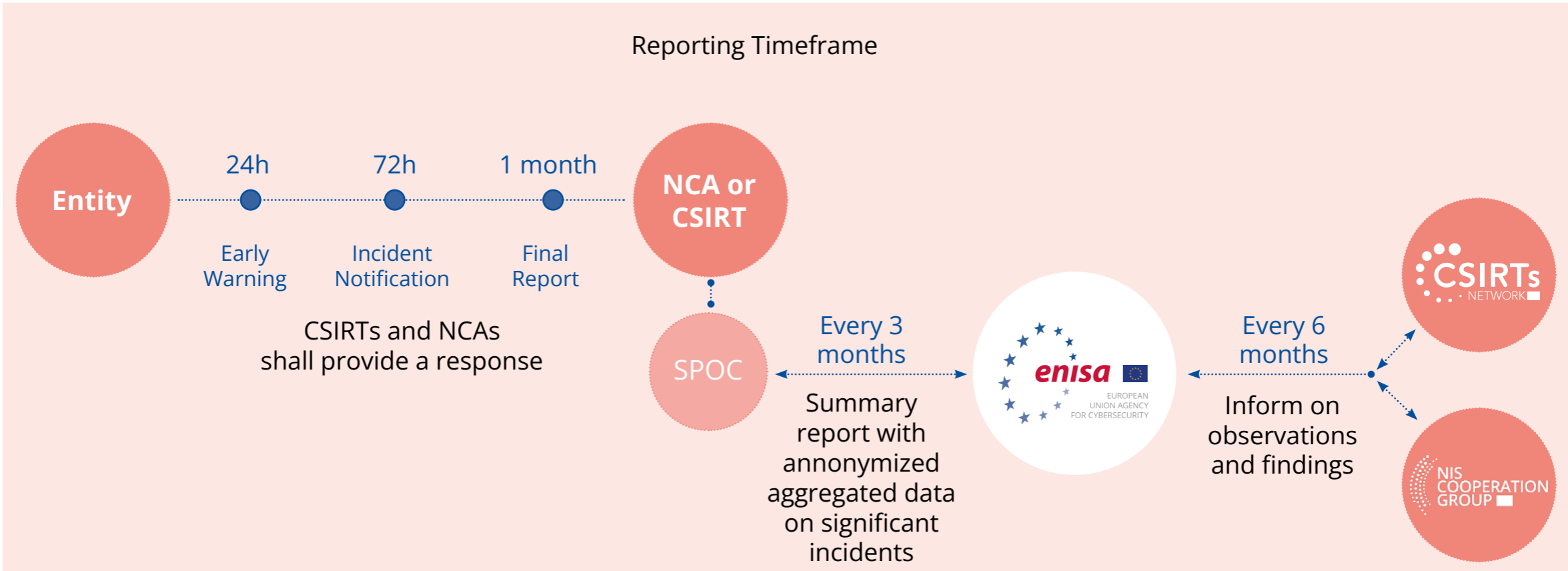
An event that has caused/could cause severe operational disruption or financial loss.




■ 2

An event that has caused or could cause damage to natural or legal persons.

■ A REPORTABLE INCIDENT HAPPENED – NOW WHAT?






■ 1


Where applicable, Member States shall ensure that entities communicate to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat.

Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.




■ 2

When in the public interest, Member states may inform the public or ask the entity to do so.



■ 3

If the significant incident concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform, the other affected Member States and ENISA.



enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

20

years!

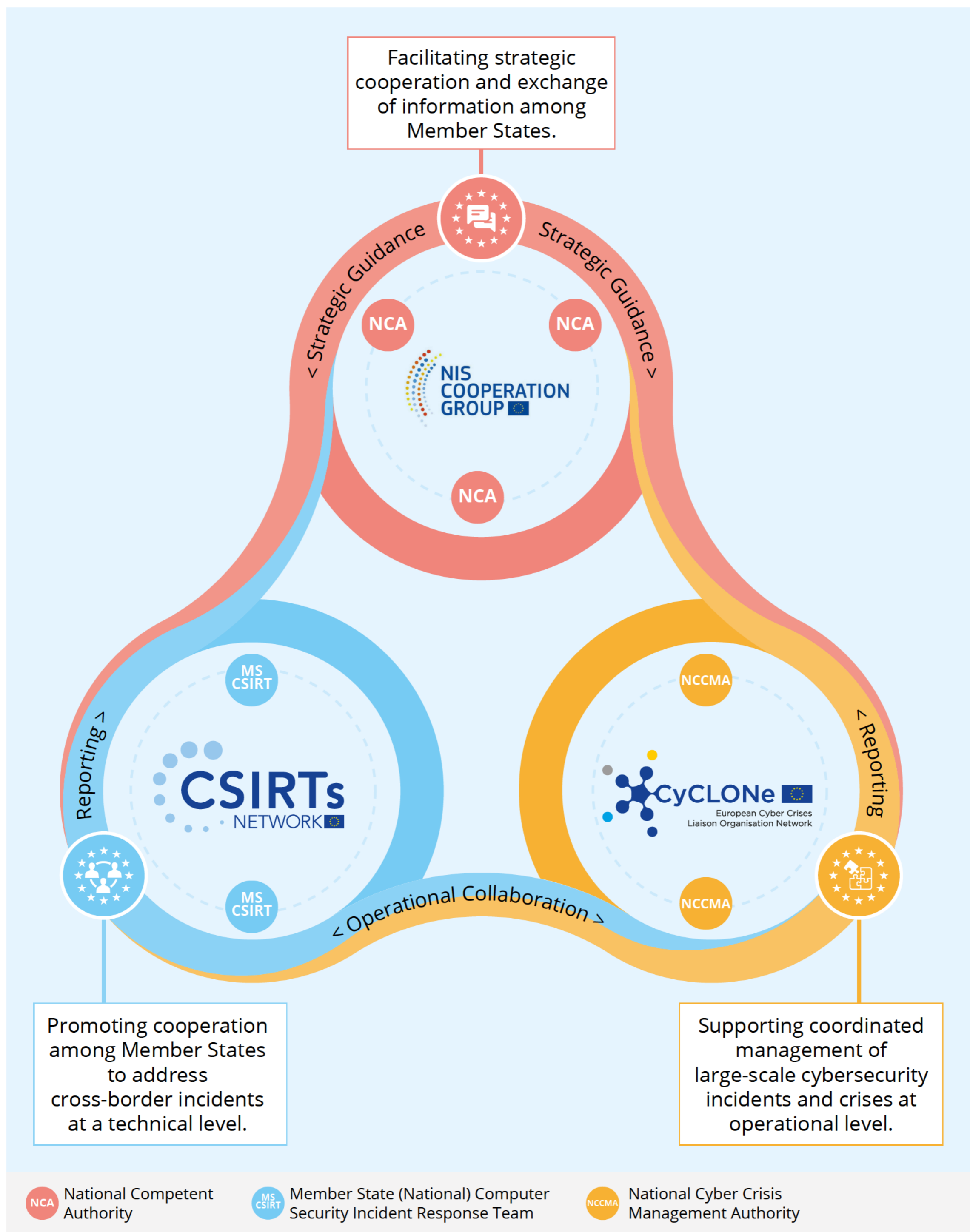
Disclaimer: The above guidelines provide a general overview of the NIS2 incident reporting framework. Member states retain the authority to define specific details and measures, which may vary.

EU-LEVEL COLLABORATION








The NIS2 Directive promotes EU-level collaboration through dedicated networks and provisions.

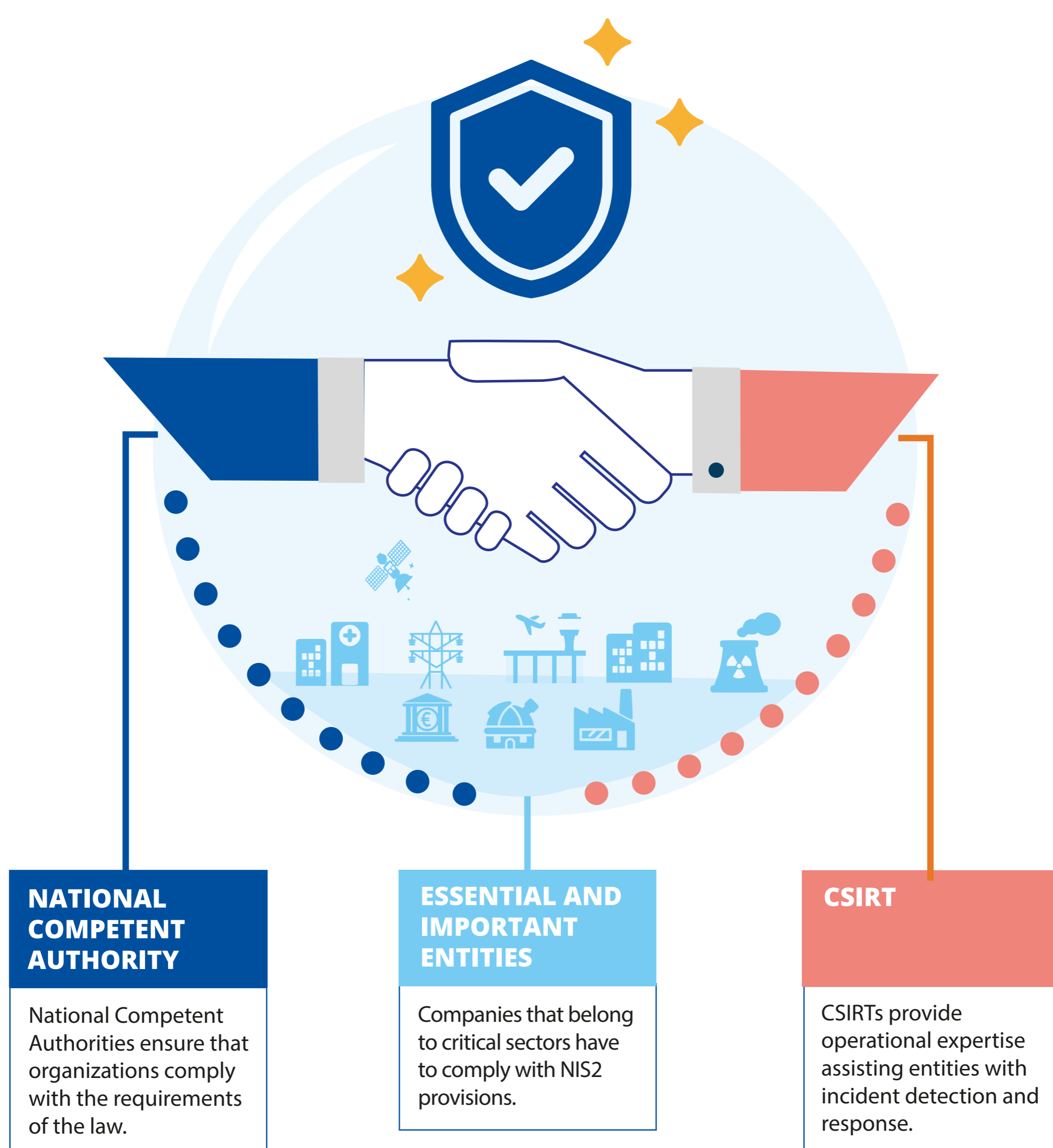
Member States participate in 3 pivotal networks each with a different mandate.



MEMBER STATES TAKE ACTION TO:

Increase cybersecurity capabilities via:		Jointly tackle challenges relevant to:							
	Peer reviews among Member States, to learn from shared experiences and achieve a high common level of cybersecurity		Mutual assistance Among Member States competent authorities for enhanced cross-border supervision.		Vulnerability Disclosure		Risk Assessments of Critical Supply Chains		Large-Scale Incident Management

SUPERVISION OF ENTITIES IN SCOPE



■ National Competent Authorities



Monitor compliance performing on-site inspections and off-site supervision either on a regular basis or ad-hoc following a significant incident or an infringement.



Receive incident reports.



Impose supervisory or enforcement measures to ensure compliance.



Collaborate with CSIRTs on technical responses to incidents.



Participate in EU-level information sharing and coordination.



Cooperate with authorities from other Member States using a mutual assistance mechanism.

■ CSIRTs



Detect, analyse and respond to cyber incidents.



Coordinate technical responses to mitigate impact.



Disseminate information about threats and vulnerabilities.



Facilitate EU cooperation and information exchange.



Enhance preparedness and awareness among entities.

■ Essential and important entities



Implement security measures.



Evidence compliance.



Report significant incidents and on a voluntary basis non-significant incidents and near-misses



The details of supervision depend on national legislation.



Essential entities are subject to a comprehensive ex ante and ex post supervisory regime, while important entities are subject to ex post only, supervisory regime.

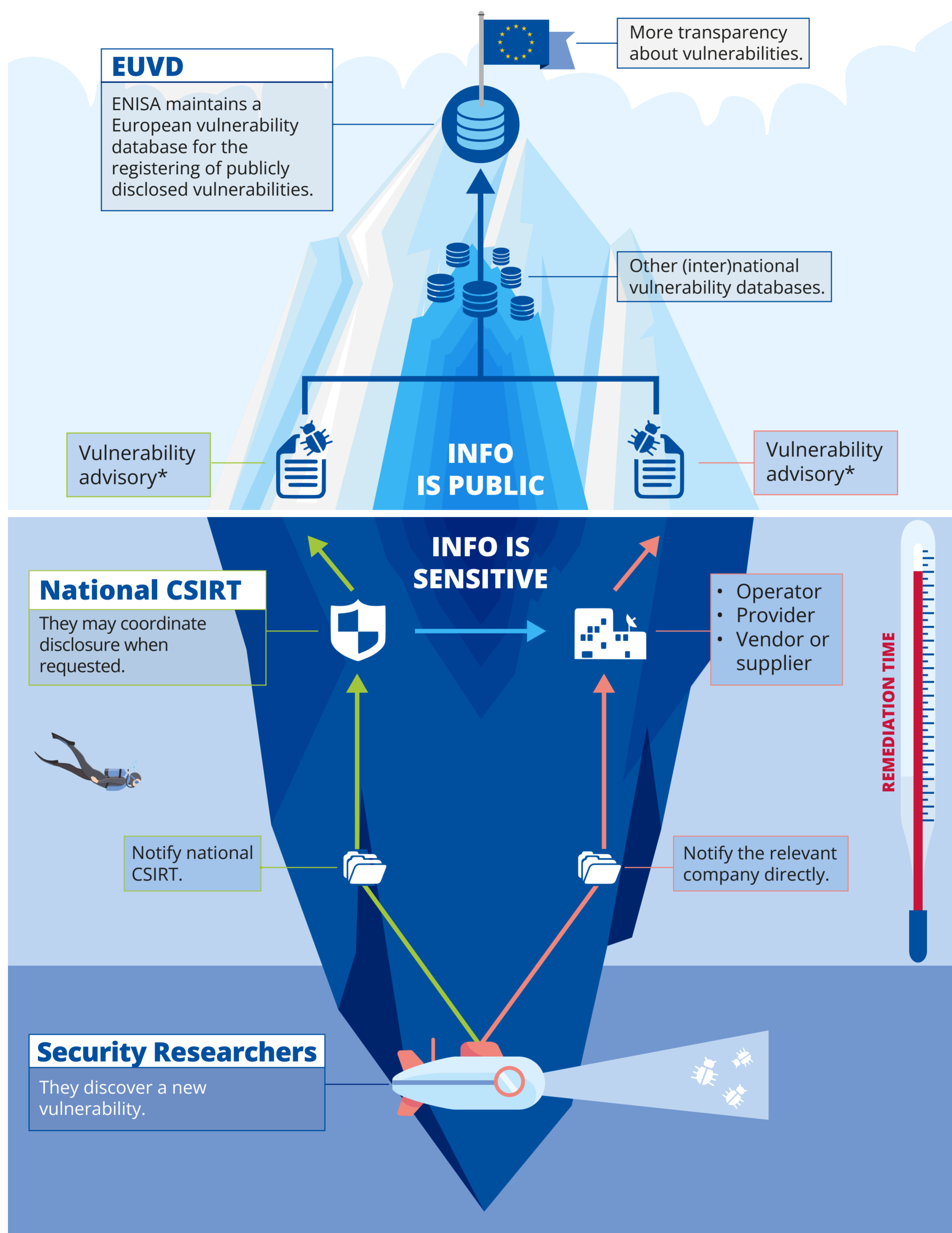


Where an entity provides services in more than one Member States, or provides services in one or more Member States and its network and information systems are located in one or more other Member States, the competent authorities of the Member States concerned shall cooperate with and assist each other as necessary, using a mutual assistance mechanism.

VULNERABILITY DISCLOSURE



NIS2 introduces Coordinated Vulnerability Disclosure, a structured disclosure process and a European database with information about disclosed vulnerabilities.



* The national CVD policy and procedure ensures disclosure is done carefully and timely, so that there is enough time for affected entities to find a patch or a solution, before it is disclosed publicly.

■ 1

A national CVD policy is required by the NIS Directive, to ensure that ethical hackers, who follow good practices, can remain protected from criminal or civil liability and prosecution.



■ 2

The NIS2 designates the national CSIRT as a coordinator between the vendor and ethical hacker, to ensure safe and timely disclosure of new vulnerabilities.



■ 3

For Member States it is important to raise awareness and promote their national CVD policy.



IMPLEMENTING REGULATION



The Implementing Regulation is a legal text that specifies EU law requirements, aiming to create **uniform conditions** across Europe for the implementation of NIS2 Directive rules. These regulations are **binding** and **directly applicable** in all **Member States**.








■ CYBERSECURITY RISK MANAGEMENT MEASURES:

The implementing regulation establishes 13 groups of technical and methodological requirements necessary for the application of the 10 NIS2 cybersecurity risk-management measures



■ REPORTING THRESHOLDS:

An incident is **considered significant** and **needs to be reported** in the following **7 situations**:

Has caused or is capable of causing:	
<div>  </div> <div> <p>■ 1</p> <p>Financial loss for the relevant entity that exceeds EUR 500 000 or 5 % of the relevant entity's annual turnover, whichever is lower</p> </div>	<div>  </div> <div> <p>■ 5</p> <p>A successful, suspectedly malicious and unauthorized access to network and information systems occurred, which is capable of causing severe operational disruption.</p> </div>
<div>  </div> <div> <p>■ 2</p> <p>The exfiltration of trade secrets</p> </div>	<div>  </div> <div> <p>■ 6</p> <p>It is a recurring incident (if it has occurred at least twice within 6 months and the root cause is the same and they collectively meet the financial damage criteria).</p> </div>
<div>  </div> <div> <p>■ 3</p> <p>The death of a natural person</p> </div>	<div>  </div> <div> <p>■ 7</p> <p>The incident meets one or more of the criteria specific for each type of entity in scope the Implementing regulation.</p> </div>
<div>  </div> <div> <p>■ 4</p> <p>A considerable damage to a natural person's health</p> </div>	

* Additional provisions determining the severity of the incident apply for the different categories of entities and are specified in the Implementing Act.

■ ENTITIES IN SCOPE:

The entities in scope of the implementing regulation require a high level of harmonization in the Member States regarding requirements for cybersecurity risk-management measures and incident reporting thresholds, due to their cross-border nature.

