KPMG

EU NIS2 Directive: Taking EU cybersecurity maturity to the next level

23 May 2023

Presenters

Hussain Ahmed

Senior Manager -
Cyber and Privacy Practice at KPMG Advisory Belgium

Hussain has a background in telecoms with over 12 years of experience in ICT regulations including data privacy and information security. He joined KPMG in 2022 where he supports clients by conducting gap assessments and developing roadmaps to help comply with ICT (Cybersecurity and Privacy) related legal and regulatory requirements, international standards and best practices.

Benoit Watteyne

Director and competence lead-
Cyber and Privacy Practice at KPMG Advisory Belgium

Benoit joined KPMG Advisory in 2007 and is currently the Competence Leader for the KPMG Cyber & Privacy Team. His team provides a wide range of services to create a resilient and trusted digital world — even in the face of evolving threats – such as cyber strategy and governance, technical engagements, such as ethical hacking and cyber incident response.

Agenda

01

Setting the Scene

EU Cybersecurity Regulatory Framework

REGULATION (EU) 2019/881 on Cybersecurity Act (CSA)

Cybersecurity Act strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services.

Directive NIS2 (EU) 2022/2555

Sets cybersecurity measures on entities falling under critical infrastructure sectors.

DORA (Digital Operational Resilience Act) – Financial sector Regulation (EU) 2022/2554

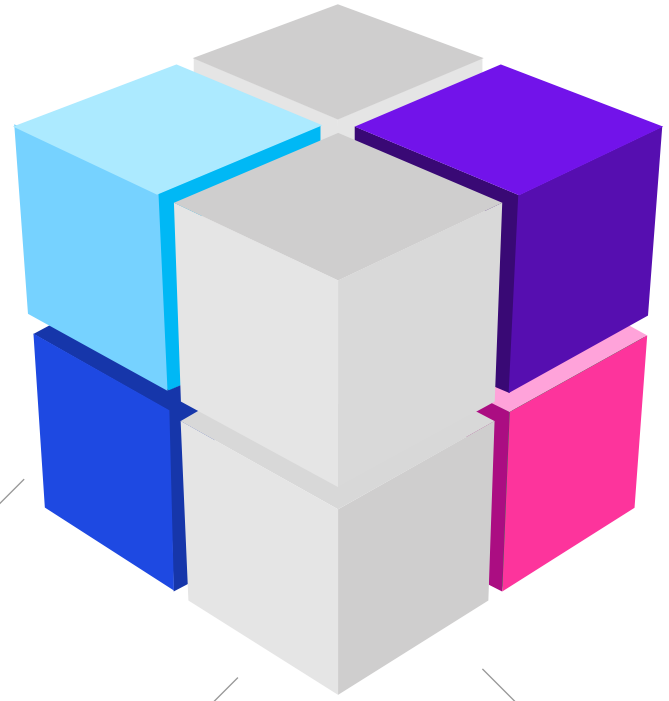
Ensures that financial entities in EU remain resilient through a severe operational disruption.

Cyber Resilience Act (proposal)

Use of EU cybersecurity certifications and rules to ensure more secure hardware and software products.

RED - radio equipment directive 2014/53/EUEN

Establishes a framework for placing radio equipment on market and subjects certain categories of radio equipment to increased level of cybersecurity, personal data protection and privacy.



Regulation (EU) 2021/887 ECCC (Network of National Coordination Centres)

Boosts research excellence and the competitiveness of the Union in the filed of cybersecurity.

Directive (EU) 2019/1937 on Whistle-blower

Reports of violations of NIS requirements

Directive CER (EU) 2022/2557 (Resilience of critical entities)

strengthens the resilience of critical infrastructure to a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage.

Network Code on sector-specific rules for cybersecurity aspects of cross border electricity flows (NCCS)

Sets a standard for cross border flows in EU.

(non exhaustive list)

Evolution of EU NIS Directive

NIS1 Directive (2016)

First piece of EU-wide horizontal legislation on cybersecurity, which was predominantly applicable to operators of essential services and digital service providers.

Transposition into National Law (2019)

Each EU member state was to implement it by May 2018; In Belgium, the law entered into force in May 2019.

NIS2 Directive Proposal (2020)

In Dec 2020, a review proposal was made by European Commission to respond to cyber threats and challenges in implementation, while ensuring uniformity across EU member states. This includes expanding the scope of NIS to cover additional sectors.

NIS2 Directive (2022)

EU Trialogue process completed (almost 24 months) and EU NIS2 directive was issued in Q4 2022.

NIS1 External Audit Reviews (2022-24)

Belgian cybersecurity authority (CCB) in coordination with sectorial competent authorities are expecting / conducting external audit reviews of organisations falling under scope of NIS1.

NIS2 Transposition into National Law (Oct 2024)

From date of its issuance in EU journal, Belgium will have 21 months to transpose it into local Belgian law. In Belgium, impacted entities are expected to comply with it starting Oct 2025 (to be confirmed).

NIS2 Compliance Assessments

Concerned entities (referred to as Essential and Important entities – EIEs, i.e. our customers) need to start preparations from now!

Highlights of NIS2

01

Issued on 27 December 2022 in EU Journal. EU member states (MSs) including Belgium are expected to transpose it within 21 months from that date.

02

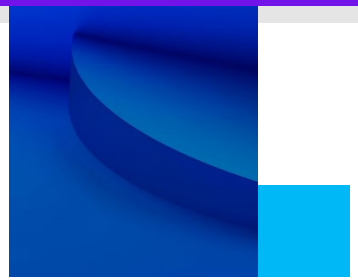
A new EU regulatory instrument which all EU MSs will have to comply with from its date of issuance.

03

NIS2 aims to protect organizations falling under critical infrastructure within EU from cyber threats by enforcing a higher level of common security practices across EU.

04

NIS2 replaced its predecessor (NIS1) due to incompatibility in level of enforcement across EU MSs and increased number of cyberattacks on critical infrastructure in EU over past few years.



05

The new directive introduces stringent security measures in relation to cybersecurity risk management including supply chain, reporting obligations, supervisory and enforcement obligations including on-site inspection and audit reviews.

02

Who does NIS2 apply to?

New terminologies: Essential and Important Entities

Essential Entities

01

- All existing entities designated as critical infrastructure under EU CER directive
- Entities listed in Annex 1 of NIS2 directive which exceed the ceilings for medium-sized enterprises as per article 2 of the Annex to Recommendation 2003/361/EC (an enterprise which employs more than 250 persons and/or has an annual turnover exceeding EUR 50 million, and/or an annual balance sheet total exceeding EUR 43 million)
- Qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size;
- Providers of public electronic communications networks or of publicly available electronic communications services
- Public administration entities:
    - central governments as defined in national law and/or
    - regional governments (based on a risk assessment at EU MS level)

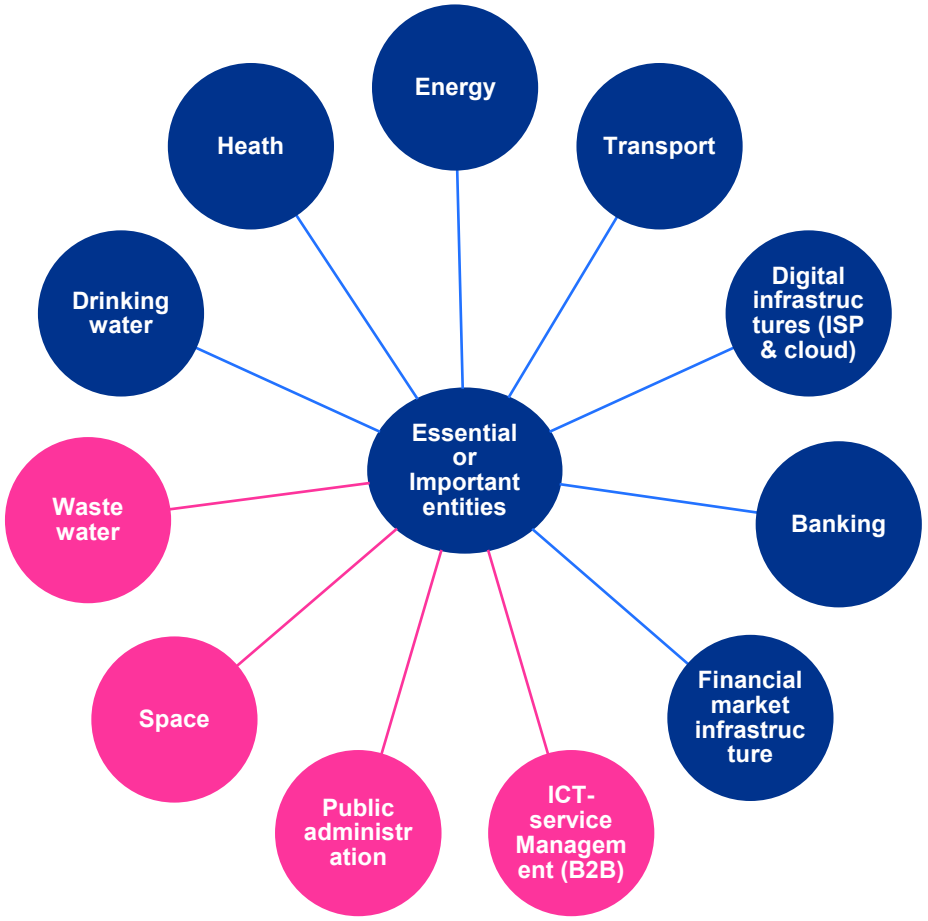
Important Entities

02

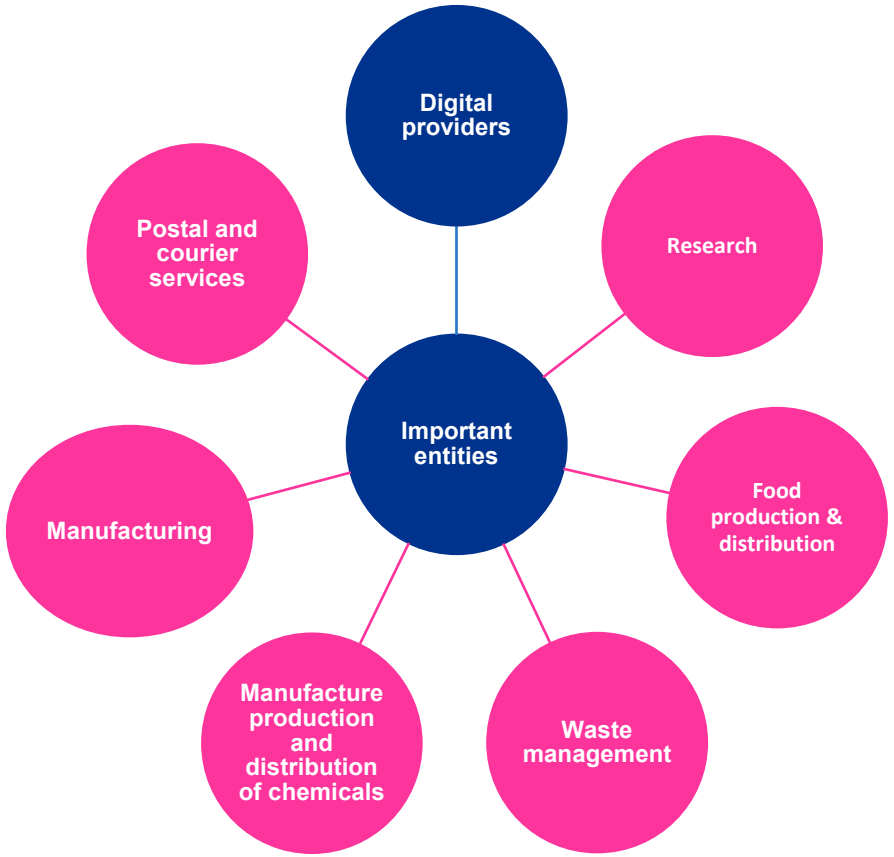
- All entities falling under scope of Annex 1 of NIS2 directive which do not meet the criteria of large enterprise as per article 2 of the Annex to Recommendation 2003/361/EC (details listed above)
- All entities which are listed in Annex 2 of NIS2 directive
- All entities as designated by EU MS based on a risk assessment

Critical Sectors divided into two lists (NIS2 Annexes 1 & 2)

Annex 1: High Criticality



Annex 2: Other Critical (Important)



NIS1 sectors are in navy blue and new sectors colored in Pink

Economic Sectors falling under scope of NIS2

CENTRE FOR CYBER SECURITY BELGIUM

NIS-2 Scope – Final version

Sector	Subsector	Jurisdiction	Critical entities (CER)	Large **at least 250 employees OR** with an annual turnover of **at least 50 million euros** (or an annual balance sheet total of at least 43 million euros)	Medium entities: **at least 50 employees OR** with an annual turnover (or balance sheet total) of **at least 10 million euros**	Small & Micro
Annex I: Sectors of high criticality						
1. **Energy**	Electricity; district Heating &cooling; Gas; Hydrogen; oil;	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as** essential or important **by national authorities** due to sole service, significant impact, essential to society
2. **Transport**	Air (commercial carriers; airports; traffic); Rail (infra and undertakings); Water (transport companies; ports; traffic services); Road (ITS & charging stations)					
	Special case: Public Transport: **only** if identified as CER					
3. **Banking**	Credit institutions **(attention: DORA lex specialis)**					
4. **Financial Market Infrastructure**	Trading venues, central counterparties **(attention: DORA lex specialis)**					
5. **Health**	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency					
	Special case: entities holding a distribution authorization for medicinal products: **only** if identified as CER					
6. **Drinking Water**						
7. Waste Water	(only if it is an essential part of their general activity)					
8. **Digital Infrastructure**	Qualified trust service providers			Essential		
	DNS service providers (excluding root name servers)	**One stop**: Only the MS where they have their main establishment				
	TLD name registries					
	Providers of public electronic communications networks	Member State in which they **provide their services**		Essential		Important, except if identified as essential based on National risk assessment
	Non-qualified trust service providers	The Member State(s) where it is established		Essential	Important, except if identified as essential by Member State	
	Internet Exchange Point providers		Essential			
	Cloud computing service providers	**One stop**: Only the MS where they have their main establishment				Not in Scope, **except if identified as** essential or important
	Data centre service providers					
	Content delivery network providers					
8a. ICT-service management (B2B)	Managed Service Providers, Managed Security Service Providers					
9. Public Administration entities	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security). Of regional governments: risk based. (Optional for Member States: of local governments)	MS that established them		Essential		
10. Space	Operators of ground-based infrastructure (by MS)	The Member State(s) where it is established		Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as** essential or important
Annex II: other critical sectors						
1. Postal and courier services		The Member State(s) where it is established	Essential	Important, except if identified as essential by Member State		Not in Scope, **except if identified as** essential or important **by national authorities** due to sole service, significant impact, essential to society
2. Waste Management	(only if principal economic activity)					
3. Chemicals	Manufacture, production, distribution					
4. Food	Production, processing and distribution					
5. Manufacturing	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)					
6. Digital providers	online marketplaces, search engines, social networking	**One stop**: Only the MS where they have their main establishment				
7. Research	Research organisations **(excluding education institutions)** (Optional for Member States: education institutions)	The Member State(s) where it is established				
Entities providing domain name registration services		**One stop**: Only the MS where they have their main establishment	*All sizes, but only subject to Article 3(3) and Article 28*			

Regulatory regimes: Essential and Important Entities

Below is a table with key differences between both categories of entities subject to NIS2 requirements (more details in subsequent slides):

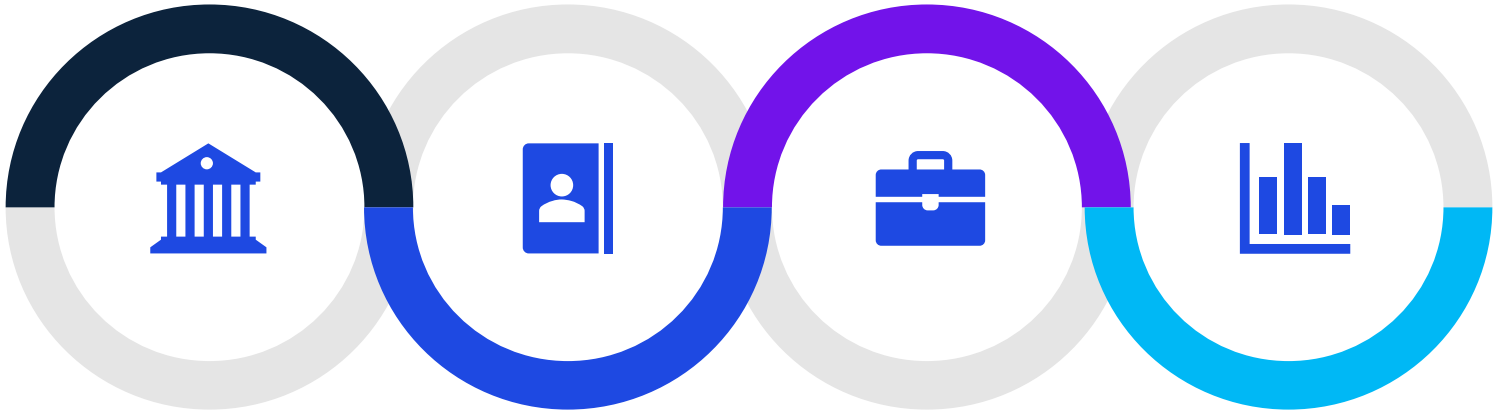
	Essential Entities	Important Entities
Security requirements	Risk based security obligations and measures: all hazard approach referenced in the legal text.	
Reporting Obligations	Significant incidents	
Supervision	Ex-ante + ex post	Ex-post
Sanctions	Minimum list of administrative sanctions including fines. Only for essential entities: ultima ratio possibility to suspend authorisation or impose temporary ban on managerial duties.	
Jurisdiction	General rule: MS where the entities are established. Exception: Telcos – MS where they provide services; certain digital infrastructure and digital providers – main established in the EU.	

03

Existing Requirements under NIS1

NIS1 Key Requirements (in Belgium)

KPMG analysed the Belgian law of 2019 transposing EU NIS1 directive and has identified key focus areas which are relevant to Operators of Essential Services (OESs):



ISO 27001

Alignment with the ISO 27001 standard or approved equivalent. Presumption of conformity when already ISO 27001 certified.

3rd parties

A robust framework needs to be put in place to define security requirements and ensure adequate governance of your 3rd parties (vendors, suppliers, sub-contractors, cloud service providers, etc.).

Incident Management

One major requirement is in relation to managing and reporting cyber security related incidents.

SPOC

Another key aspect is designating a Single Point of Contact within the organisation who shall be responsible for liaising with competent authorities for cyber security matters.

Understanding NIS1 requirements (enforced at present)

Key Security requirements for Operators with Essential Services (OES)

01 Define an information security policy.

02 Provide a description of the network and information systems they depend on.

03 Take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risks posed.

04 Take appropriate measures to prevent and minimise the impact of incidents.

05 Designate a contact point with competent authorities.

06 Incident notification to competent authorities (if personal data is involved (e.g. employee data or individual clients personal data) —> notify Belgian Data Protection Authority (no later than 72 hours from being aware of incident).

07 Conduct a yearly internal audit and a three-yearly external audit for Operators of Essential Services (OES). ISO27001 certification can be used as an equivalence to fulfil this requirement.

04

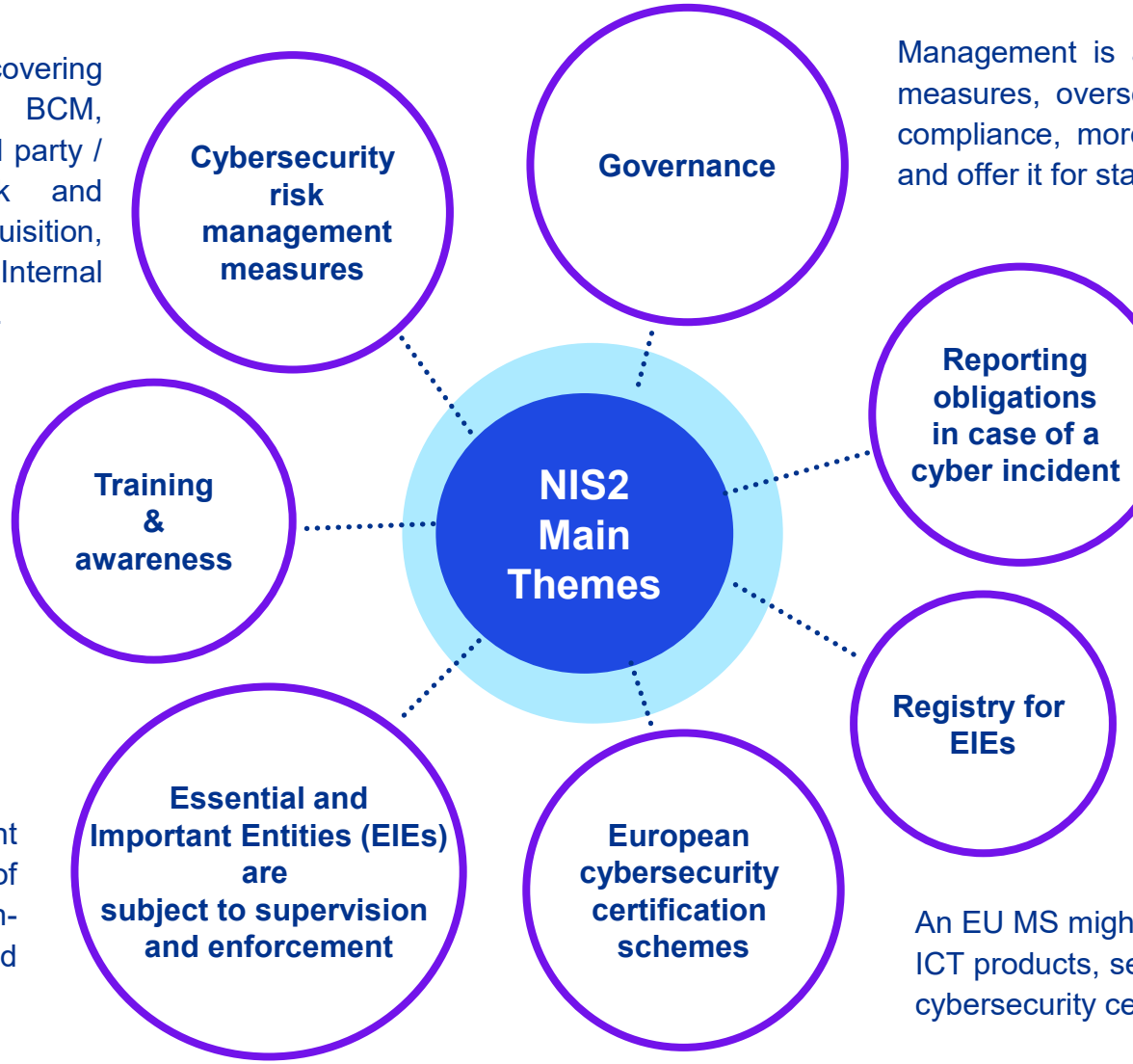
New Requirements under NIS2

NIS2 - High Level Overview of Requirements

Measures include security policies covering IS, HR, MFA, Assets, Access, BCM, Incident response and reporting, 3rd party / supply chain security, Network and Information Systems acquisition, development & maintenance, and Internal Audit (detailed in subsequent slides).

An entity is required to ensure that all staff at different levels receive regular cybersecurity training and have necessary skills to identify and assess cyber related risks and implement adequate measures.

This includes providing competent authorities with evidence of compliance including facilitating on-site inspections, audit visits and reviews.



Management is accountable for approving cybersecurity measures, oversee the implementation and be liable for compliance, moreover, management is to follow training and offer it for staff on regular basis.

In case of an incident or significant cyber threat, an entity must notify the competent authorities / CSIRT within a set timelines (detailed in subsequent slides).

Upon self assessment, an entity must submit necessary information to national competent authorities and report any changes.

An EU MS might oblige entities falling under scope to use ICT products, services and processes that fulfil European cybersecurity certification schemes.

NIS2 – Cybersecurity Risk Management Measures

01

Policies on Information Security and Risk Management

02

Incident Management and Reporting

03

Business Continuity and Disaster Recovery

04

3rd Party / Supply chain security management

05

Security of network and IS acquisition, development & maintenance and vulnerability management

06

Information Security Internal Audit

07

Cybersecurity training and awareness

08

Policy on use of cryptography

09

Policies on HR, Access and Asset Management Security

10

Policy on use of Multi-Factor Authentication

NIS2 – Reporting Obligations for Cybersecurity Incidents

According to NIS2 Directive, an incident shall be considered as significant if:
(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

1. Initial Warning

Within 24 hours of becoming aware of a significant incident, an early warning shall be sent to competent authorities (via CSIRT) with initial assessment (trigger potential impact).

3. Intermediary Report (case by case)

Upon request of CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates shall be provided within set timeframes.

2. Incident Notification

Within 72 hours of becoming aware of the significant incident, an incident notification including an initial assessment of the incident, its severity and impact, as well as, where available, the indicators of compromise. For breaches with impact on personal data, GDPR rules apply.

4. Final Report

Within a month from the incident, a final report shall be submitted to CSIRT / competent authority. **Content:**

- ✓ A detailed description of the incident, including its severity and impact
- ✓ The type of threat or root cause that is likely to have triggered the incident,
- ✓ Applied and ongoing mitigation measures,
- ✓ Where applicable, the cross-border impact of the incident.

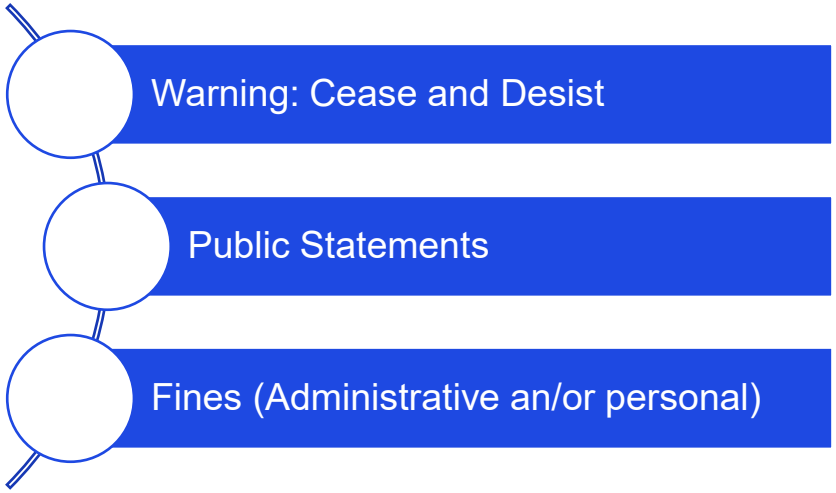
Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat.

NIS2 - New Supervisory & Enforcement Powers

Supervisory / Enforcement Measures

- An entity is a subject of on-site inspections and off-site supervision, including random checks based on risk assessment or risk-related information.
- An entity is a subject of security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria
- An entity could be asked to provide
  - necessary documentation to assess adopted cybersecurity measures including proof the implementation of IS polices
  - access to data, documents or any information necessary for the performance of their supervisory tasks.
  - evidence of implementation of cybersecurity policies.

Measures against non-compliance



Fines

- An **essential entity** may be fined up to administrative fines of **a maximum of at least EUR 10 M** or of **a maximum of at least 2 %** of the total **worldwide annual turnover**
- An **important entity** may be fined up to administrative fines of **a maximum of at least EUR 7 M** or of **a maximum of at least 1,4 %** of the total **worldwide annual turnover**

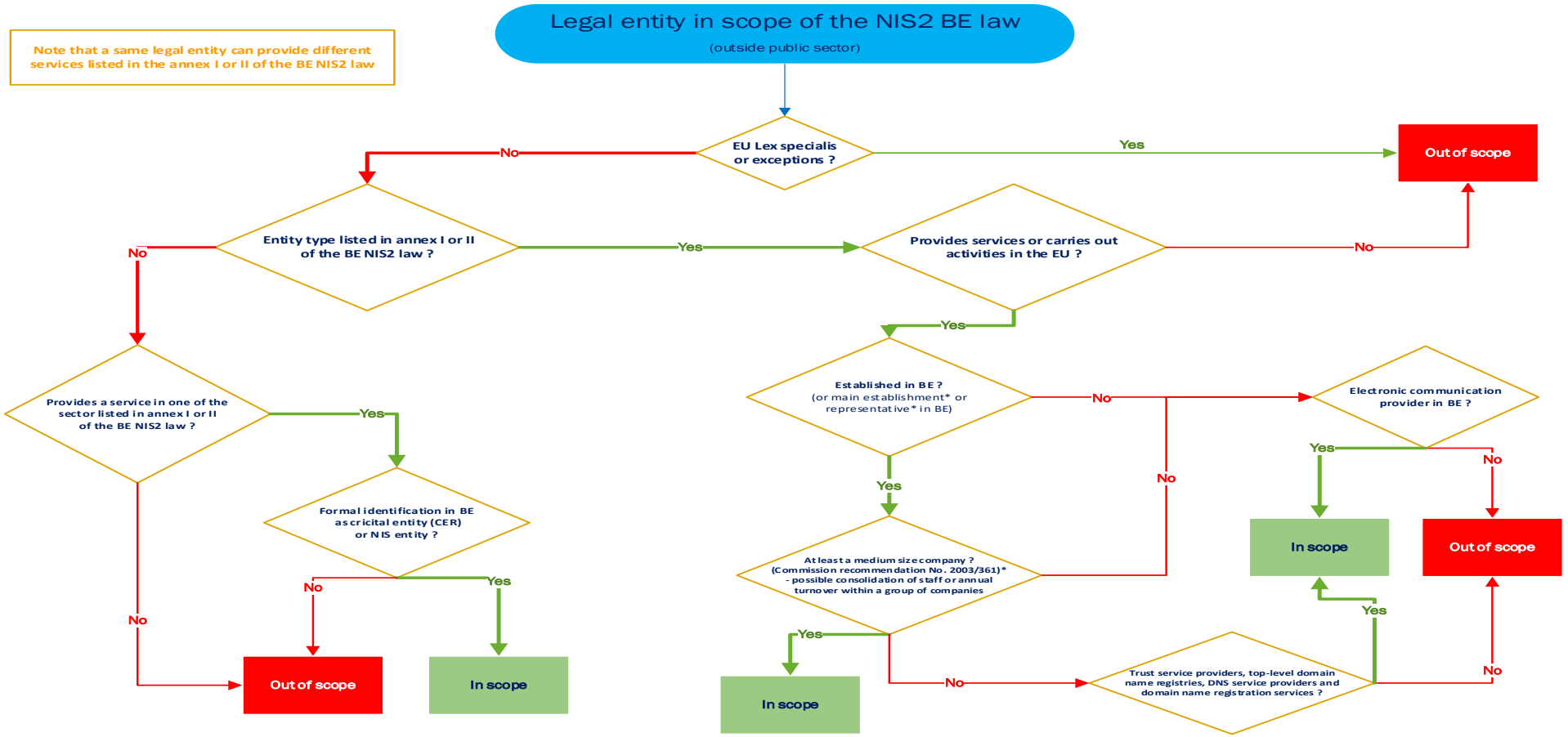
Persons responsible for entities could be hold liable (art 32.6)

Could be periodic (repeated / on-going)

05

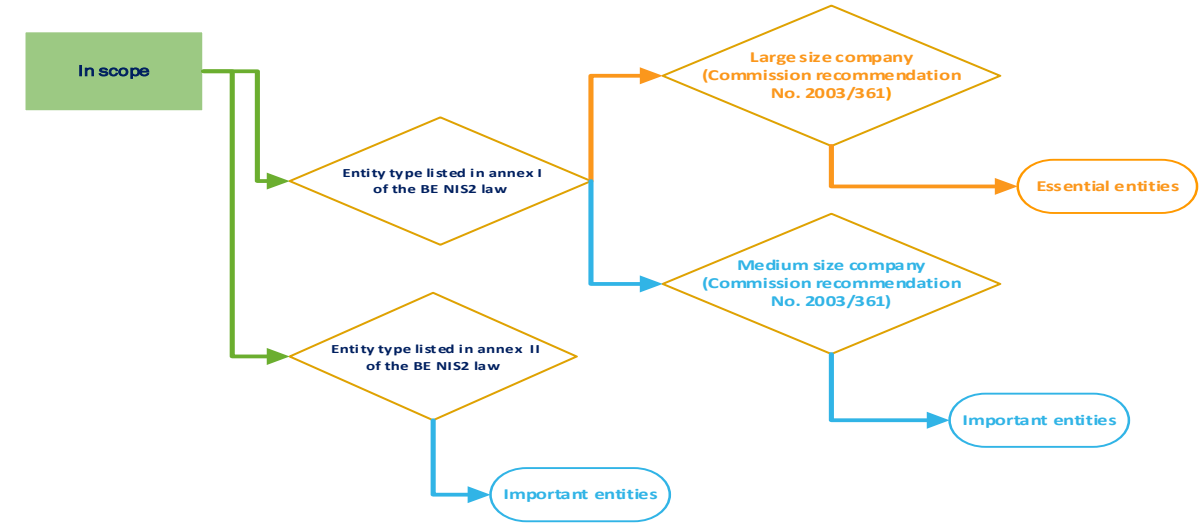
Views on way forward (based on CCB guidance)

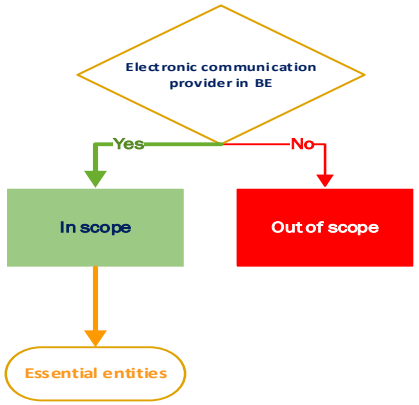
How to determine if in scope of NIS2?

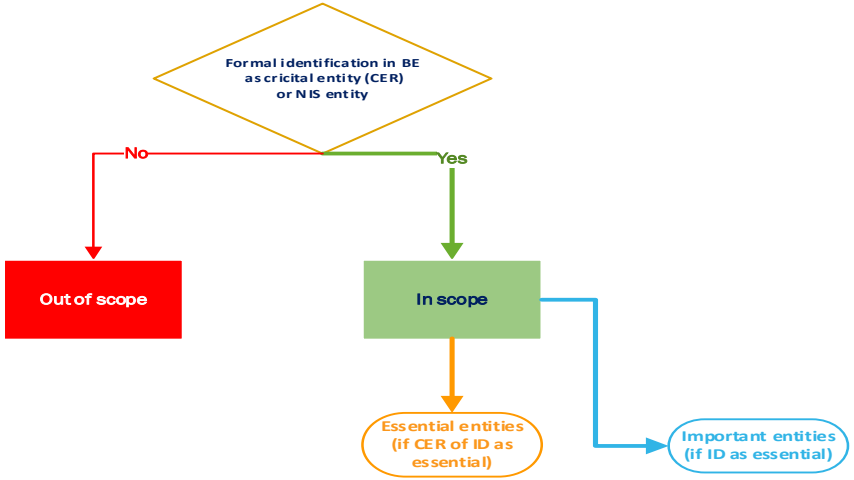


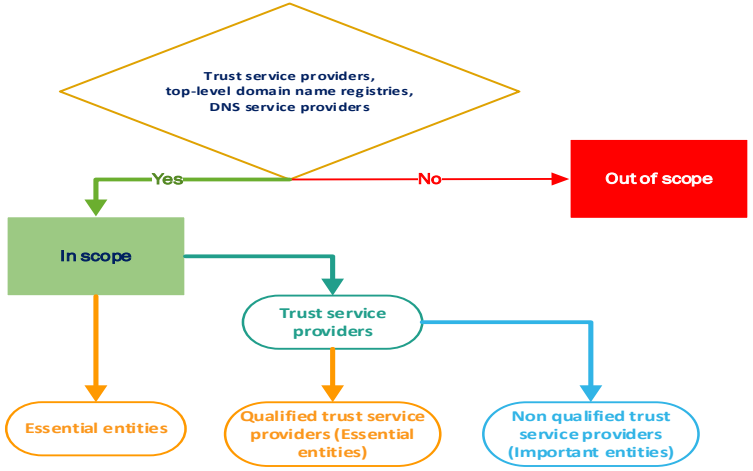
Source: Centre for Cybersecurity in Belgium, CCB

How to determine if in scope of NIS2?









Source: Centre for Cybersecurity in Belgium, CCB

Three paths to choose from (to be confirmed)

Option 1

Cyber Fundamentals

Sectoral additional requirements

Cyber Fundamentals

CENTRE FOR CYBER SECURITY BELGIUM

by an accredited CAB: ESSENTIAL (Certification) or BASIC/ IMPORTANT (Label)

Option 2

ISO27001

Sectoral additional requirements

ISO 27001 Certification by an accredited CAB

ISO 27001

Option 3

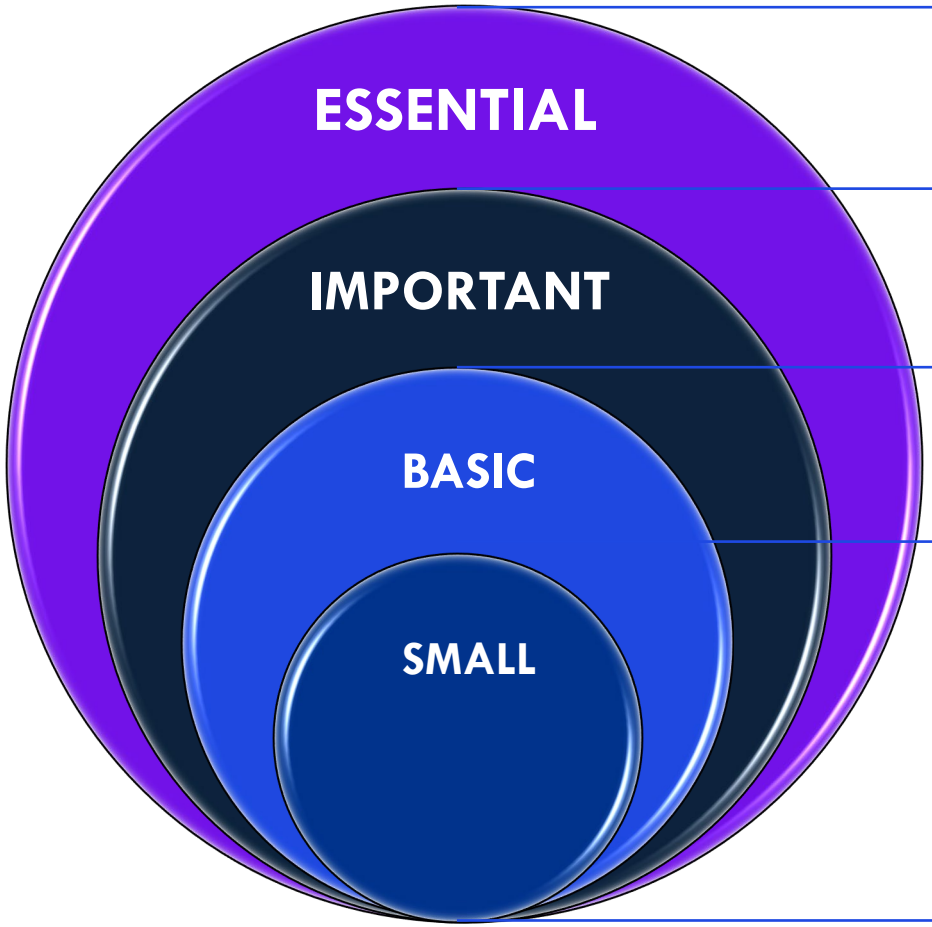
Sectorial

Equivalent sectoral regular audits/inspection

Source: Centre for Cybersecurity in Belgium, CCB

CCB Cyber Fundamental Framework

- Based on 4 frameworks: NIST CSF, ISO 27001/27002, CIS Controls and IEC 62443
- Based on our historical data, retro-fitting was done on successful cyber-attacks:
  - Assurance level **BASIC** ➔ cover 82% of the attacks
  - Assurance level **IMPORTANT** ➔ cover 94 % of the attacks
  - Assurance level **ESSENTIAL** ➔ cover 100% of the attacks
- Key measures were identified at each assurance level



144 controls

107 controls

34 controls

Non-technical formulated guidelines and recommendations

Framework:
- **Controls** (Requirements)
- **Guidance**
- **Normative references:**
  - *NIST CSF*
  - *ISO 27001/2*
  - *IEC 62443*
  - *CIS Controls*

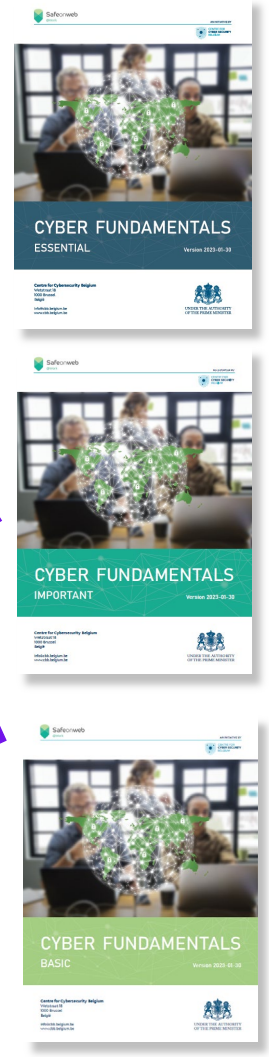
Equivalence for ISO27001 certification
(Cfr NIS 1)

Source: Centre for Cybersecurity in Belgium, CCB

CCB Cyber Fundamental Framework

Essential Entities

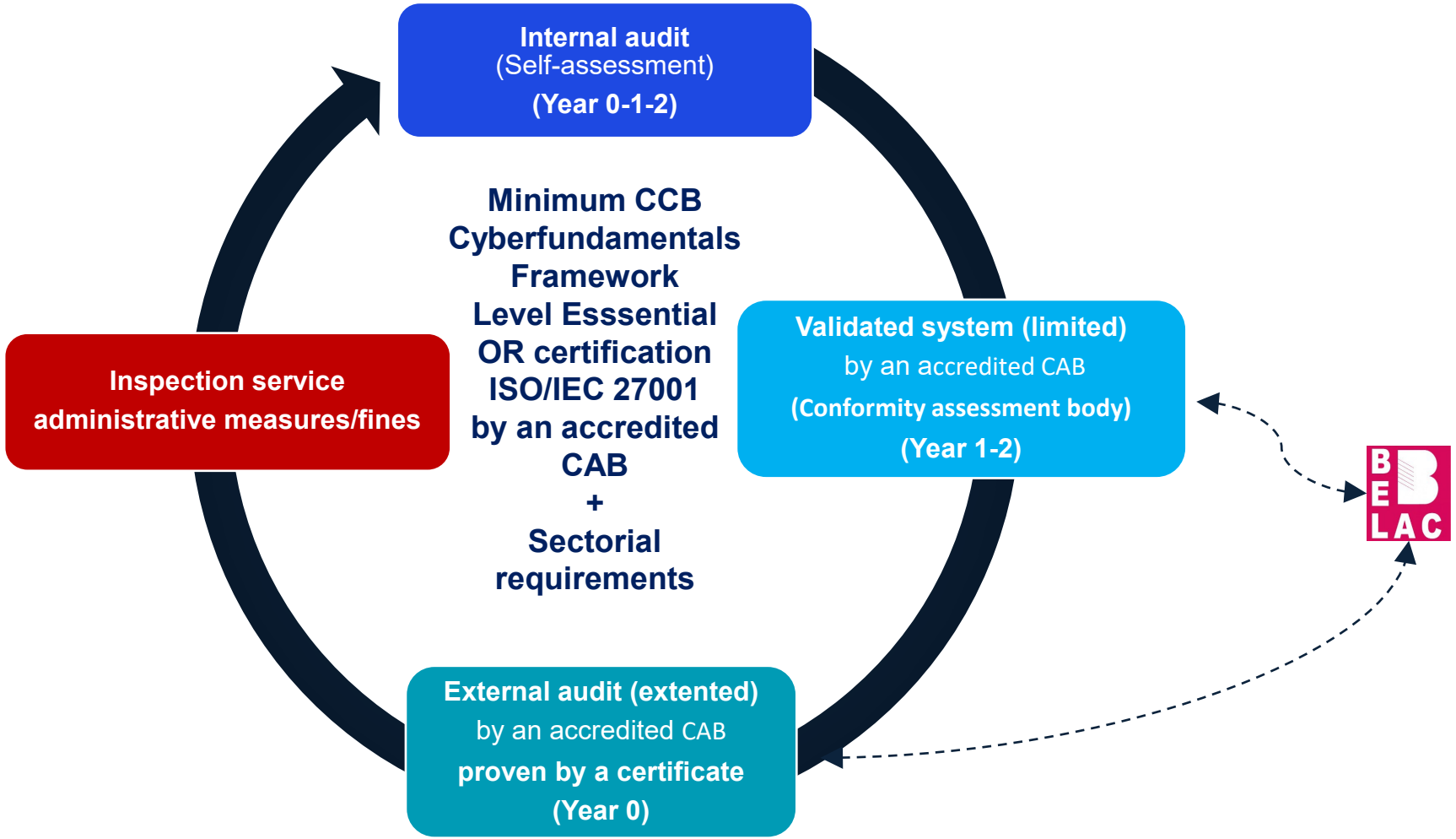
Important Entities



Entities can based on their risk analysis/assessment apply a lower level as long as the NIS2 security measures are fullfilled

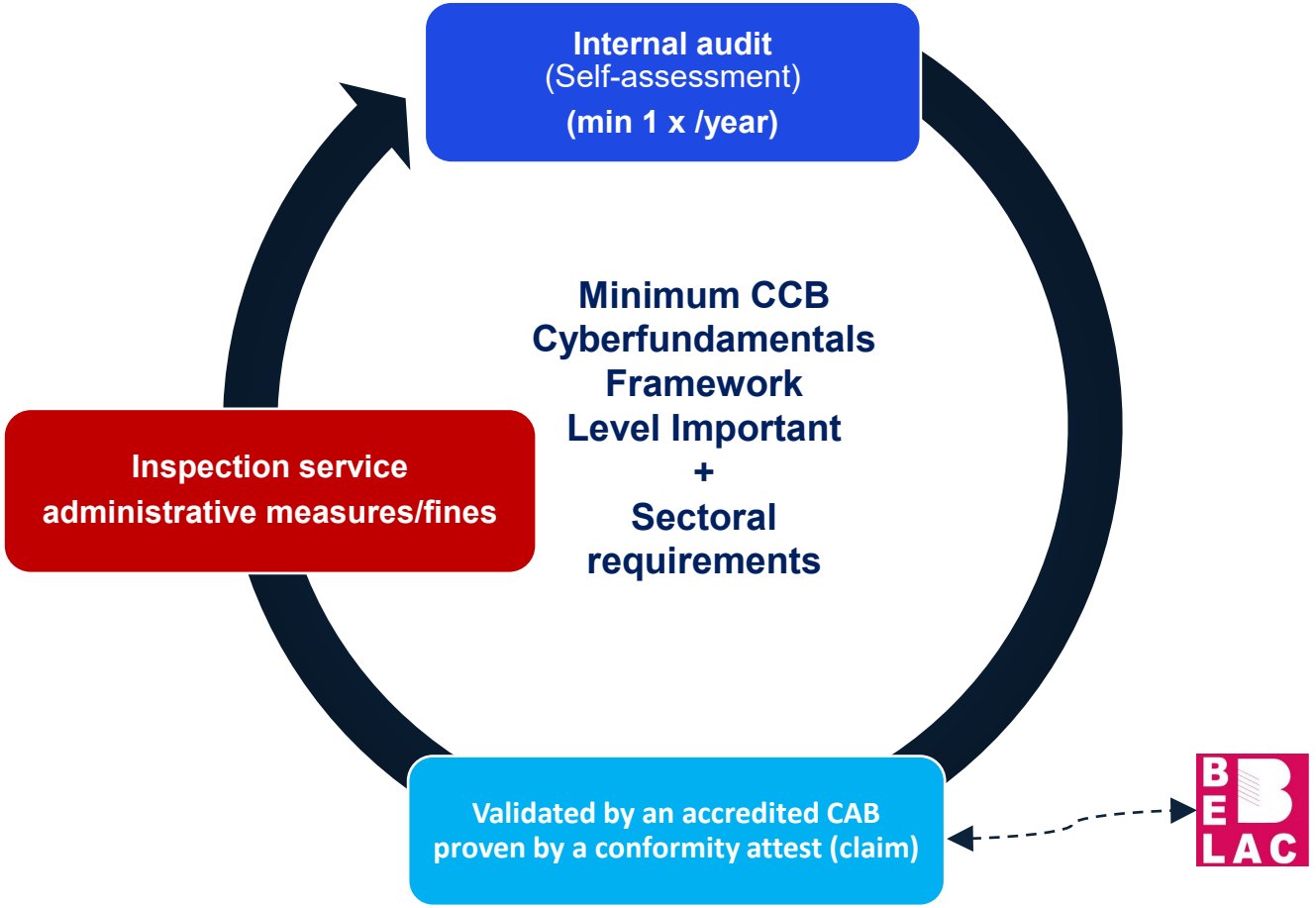
Source: Centre for Cybersecurity in Belgium, CCB

Supervision of Essential Entities in Belgium (to be confirmed)



Source: Centre for Cybersecurity in Belgium, CCB

Supervision of Important Entities in Belgium (to be confirmed)



Source: Centre for Cybersecurity in Belgium, CCB

06

How can KPMG support?

Challenges our Clients face

Defining their NIS1/2 scope

Struggling in defining the customer journey, the operational journey, security and IT services.

Awareness and education

Cybersecurity is not easy to infuse, specifically for ISO 27001 and audits.

Mobilizing resources

Right financial, human and technical resources is key!

Finding the right balance

A balance needs to be found:

1. Organizational measures vs. Technical measures
2. Time vs. Cost

Defining the scope is the key to find balance.

Change management

Adapting processes to the requirement of cyber security.

NIS made them better and stronger

1. They made transversal objectives.
2. They have a higher maturity now.
3. They implemented adaptive controls.

KPMG supports clients overcome NIS challenges

Managing Regulatory Complexity

Translated legal and regulatory text into easy to comprehend security controls that can be easily implemented by concerned teams within the organization.

Identifying Critical Digital Assets and Networks

Defined criteria to determine which ICT assets are to be deemed critical and thus, ensure that defined security compliance controls are adequately implemented.

Reporting Incidents to Competent Authorities

Defined procedures for incidence response and reporting that included designating a SPOC within the organization and means for capturing all critical incidents.

Options for Compliance

Depending on proportionality principle, risk appetite and available resources, provided clients with options for compliance

Prioritization

Supported clients prioritize actions and activities, grouped them into sub projects with defined timelines.

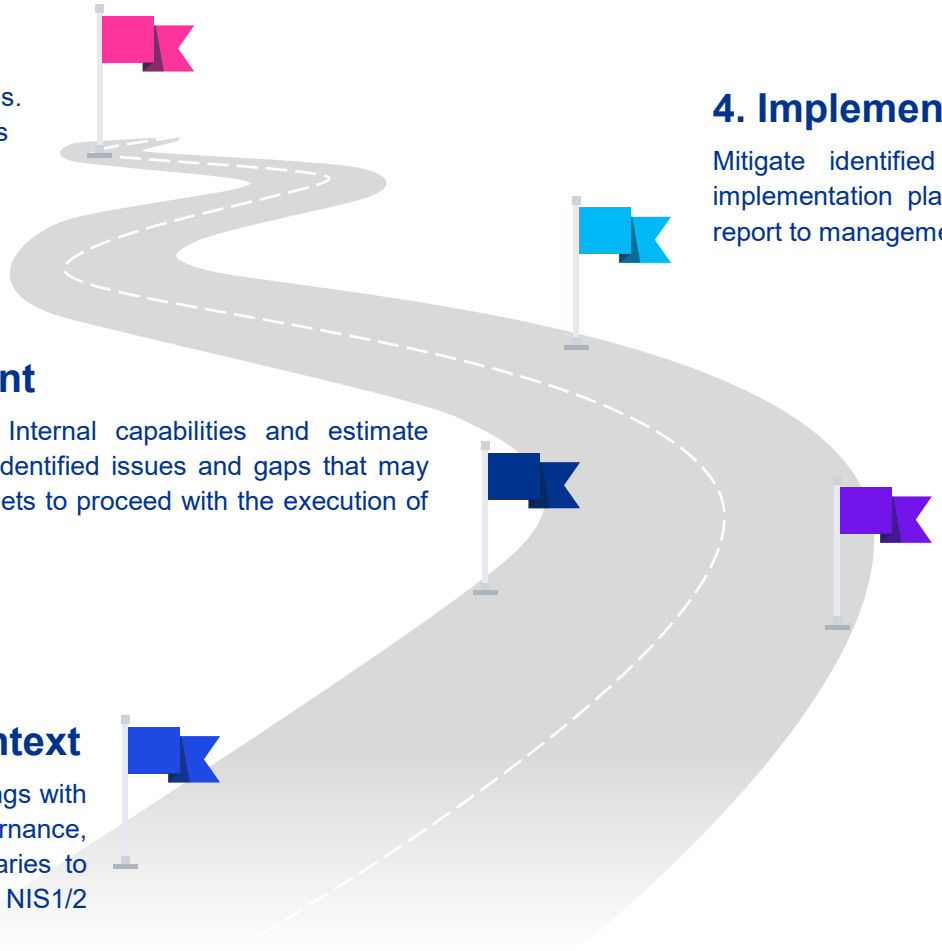
Managing Suppliers & Contractors

Defined 3rd party security risk management framework requirements. This included requirements for supply chain.

Option 1: Support clients comply with NIS1/2

5. On-going Evaluation

Continue to evaluate the progress and outcome of implementing all proposed actions, controls and initiatives. Moreover, continue to give feedback and deduce lessons learnt to enhance the execution.



4. Implementation

Mitigate identified issues and gaps by executing the agreed implementation plans. Continue monitoring the implementation and report to management on progress and concerns as applicable.

3. Capability Assessment

Support Client assess its existing Internal capabilities and estimate required resources to help address identified issues and gaps that may require allocation of resources / budgets to proceed with the execution of developed implementation plans.

2. Gap assessment

Perform a gap analysis based on requirements detailed in KPMG NIS1/2 control matrix which is based on EU NIS1/2 directive requirements mapped to ISO27001:2013 controls, taking into account risk appetite, available resources and defined objectives of Client. The analysis results into a roadmap with detailed recommendations and implementation plan(s).

1. Preparation and Establishing Context

Identify scope, objectives and end-game. Conduct meetings with relevant stakeholders of Client and setup project governance, priorities and timelines. Confirm the scope and boundaries to develop cybersecurity roadmap that shall address NIS1/2 requirements including available resources.

Option 2: Assess compliance with NIS1/2 (Audit Review)

As KPMG Certification (BE) is accredited by BELAC (the Belgian Accreditation Institute) to issue ISO 27001 certificates, our firm can help organizations falling under scope to assess their level of compliance with NIS1/2 requirements:

01 Kick off

During the kick off phase of KPMG's NIS audit, stakeholders and relevant parties are identified. Exact scope of audit is to be agreed along with timelines and resources / requirements to be made available before and during the audit.

02 Assess

Perform a through assessment of all personnel, systems and processes that fall within the scope of NIS audit based on a predefined set of controls that are detailed into Belgian law transposing NIS directive (the set of controls also include ISO27001 controls).

03 Site visits

Based on agreed scope of NIS audit, KPMG will inspect physical and environmental security measures related to information security at your organization

04 Reporting

Once all evidence is presented and systems walkthrough are completed, a comprehensive report on the audit will be handed over to your organization

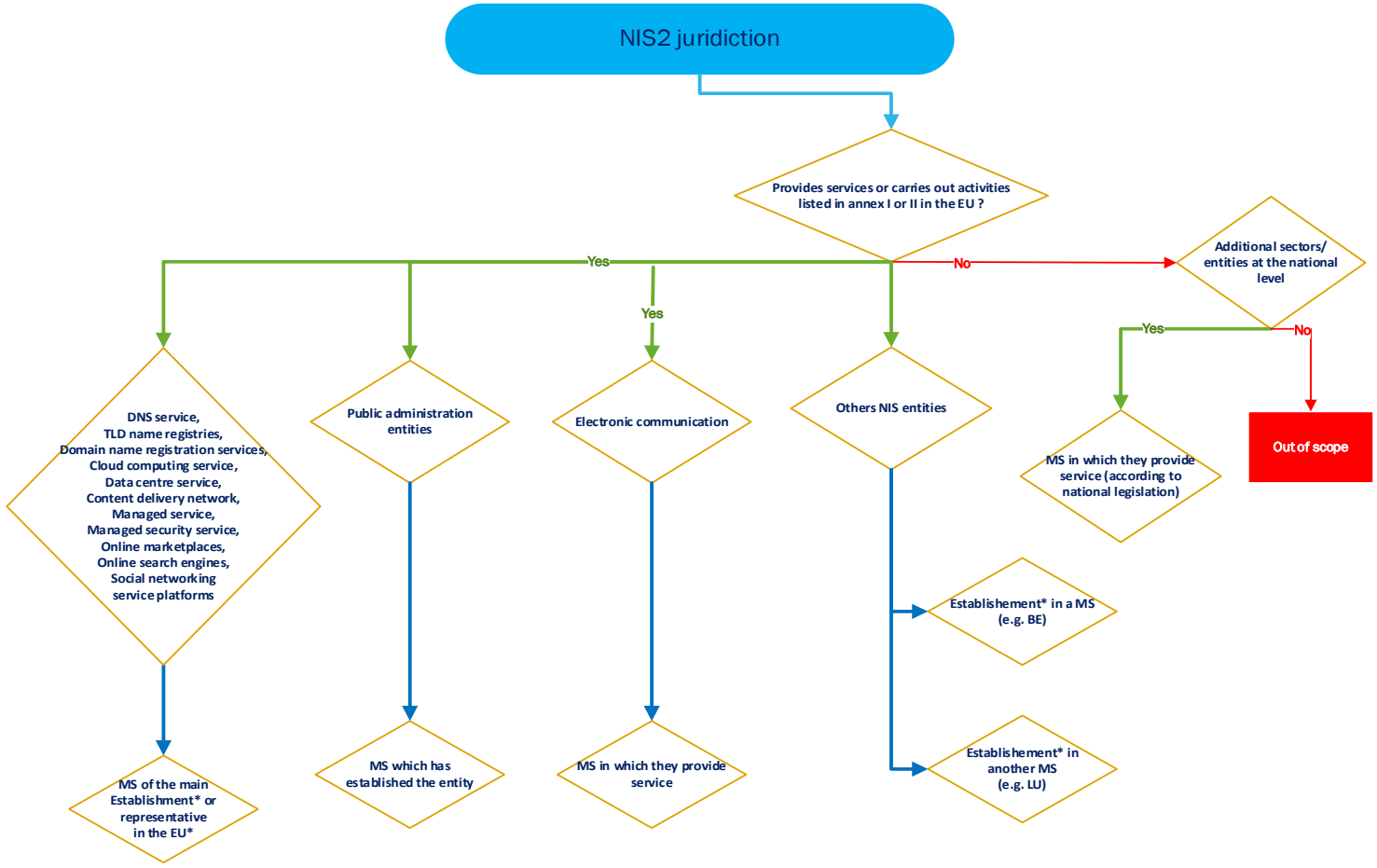
05 Follow up & Closing off

A proper closing phase in which KPMG provides your organization with the various deliverables and a comprehensive management summary guarantees the audit's quality.

NIS Control Matrix

Q&A session

How to establish jurisdiction for international companies?



Source: Centre for Cybersecurity in Belgium, CCB

Sectors overview - SECTORS OF HIGH CRITICALITY (Annex 1 / NIS2)

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	▪ Electricity undertakings as defined in Article 2, point (57), of Directive (EU) 2019/944 of the European Parliament and of the Council(1), which carry out the function of 'supply' as defined in Article 2, point (12), of that Directive ▪ Distribution system operators as defined in Article 2, point (29), of Directive (EU) 2019/944 ▪ Transmission system operators as defined in Article 2, point (35), of Directive (EU) 2019/94 ▪ Producers as defined in Article 2, point (38), of Directive (EU) 2019/944 ▪ Nominated electricity market operators as defined in Article 2, point (8), of Regulation (EU) 2019/943 of the European Parliament and of the Council(2) ▪ Market participants as defined in Article 2, point (25), of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined in Article 2, points (18), (20) and (59), of Directive (EU) 2019/944 ▪ Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider
	(b) District heating and cooling	• Operators of district heating or district cooling as defined in Article 2, point (19), of Directive (EU) 2018/2001 of the European Parliament and of the Council
	(c) Oil	• Operators of oil transmission pipelines • Operators of oil production, refining and treatment facilities, storage and transmission
	(d) Gas	• Supply undertakings as defined in Article 2, point (8), of Directive 2009/73/EC of the European Parliament and of the Council(5) • Distribution system operators as defined in Article 2, point (6), of Directive 2009/73/EC • Transmission system operators as defined in Article 2, point (4), of Directive 2009/73/EC • Storage system operators as defined in Article 2, point (10), of Directive 2009/73/EC • LNG system operators as defined in Article 2, point (12), of Directive 2009/73/EC • Natural gas undertakings as defined in Article 2, point (1), of Directive 2009/73/EC • Operators of natural gas refining and treatment facilities
	(e) Hydrogen	• Operators of hydrogen production, storage and transmission

Sectors overview - SECTORS OF HIGH CRITICALITY

Sector	Subsector	Type of entity
2. Transport	(a) Air	▪ Air carriers as defined in Article 3, point (4), of Regulation (EC) No 300/2008 used for commercial purposes ▪ Airport managing bodies as defined in Article 2, point (2), of Directive 2009/12/EC of the European Parliament and of the Council(6), airports as defined in Article 2, point (1), of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council(7), and entities operating ancillary installations contained within airports ▪ Traffic management control operators providing air traffic control (ATC) services as defined in Article 2, point (1), of Regulation (EC) No 549/2004 of the European Parliament and of the Council
	(b) Rail	• Infrastructure managers as defined in Article 3, point (2), of Directive 2012/34/EU of the European Parliament and of the Council • Railway undertakings as defined in Article 3, point (1), of Directive 2012/34/EU, including operators of service facilities as defined in Article 3, point (12), of that Directive
	(c) Water	• Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council(10), not including the individual vessels operated by those companies • Managing bodies of ports as defined in Article 3, point (1), of Directive 2005/65/EC of the European Parliament and of the Council(11), including their port facilities as defined in Article 2, point (11), of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports • Operators of vessel traffic services (VTS) as defined in Article 3, point (o), of Directive 2002/59/EC of the European Parliament and of the Council
	(d) Road	• Road authorities as defined in Article 2, point (12), of Commission Delegated Regulation (EU) 2015/962(13)responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity • Operators of Intelligent Transport Systems as defined in Article 4, point (1), of Directive 2010/40/EU of the European Parliament and of the Council

Sectors overview - SECTORS OF HIGH CRITICALITY

Sector	Subsector	Type of entity
3. Banking		▪ Credit institutions as defined in Article 4, point (1), of Regulation (EU) No 575/2013 of the European Parliament and of the Council
4. Financial market infrastructures		▪ Operators of trading venues as defined in Article 4, point (24), of Directive 2014/65/EU of the European Parliament and of the Council ▪ Central counterparties (CCPs) as defined in Article 2, point (1), of Regulation (EU) No 648/2012 of the European Parliament and of the Council
5. Health		▪ Healthcare providers as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council(18) ▪ EU reference laboratories referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council(19) ▪ Entities carrying out research and development activities of medicinal products as defined in Article 1, point (2), of Directive 2001/83/EC of the European Parliament and of the Council(20) ▪ Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 ▪ Entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list) within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council(21)
6. Drinking water		▪ Suppliers and distributors of water intended for human consumption as defined in Article 2, point (1)(a), of Directive (EU) 2020/2184 of the European Parliament and of the Council(22), excluding distributors for which distribution of water for human consumption is a non- essential part of their general activity of distributing other commodities and goods
7. Waste water		▪ Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water as defined in Article 2, points (1), (2) and (3), of Council Directive 91/271/EEC(23), excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity

Sectors overview - SECTORS OF HIGH CRITICALITY

Sector	Subsector	Type of entity
8. Digital infrastructure		▪ Internet Exchange Point providers ▪ DNS service providers, excluding operators of root name servers ▪ TLD name registries ▪ Cloud computing service providers ▪ Data centre service providers ▪ Content delivery network providers ▪ Trust service providers ▪ Providers of public electronic communications networks ▪ Providers of publicly available electronic communications services
9. ICT service management (business-to-business		▪ Managed service providers ▪ Managed security service providers
10. Public administration		▪ Public administration entities of central governments as defined by a Member State in accordance with national law ▪ Public administration entities at regional level as defined by a Member State in accordance with national law
11. Space		▪ Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks

Sectors overview - OTHER CRITICAL SECTORS

Sector	Subsector	Type of entity
1. Postal and courier services		▪ Postal service providers as defined in Article 2, point (1a), of Directive 97/67/EC, including providers of courier services
2. Waste management		▪ Undertakings carrying out waste management as defined in Article 3, point (9), of Directive 2008/98/EC of the European Parliament and of the Council(1), excluding undertakings for whom waste management is not their principal economic activity
3. Manufacture, production and distribution of chemicals		▪ Undertakings carrying out the manufacture of substances and the distribution of substances or mixtures, as referred to in Article 3, points (9) and (14), of Regulation (EC) No 1907/2006 of the European Parliament and of the Council(2)and undertakings carrying out the production of articles, as defined in Article 3, point (3), of that Regulation, from substances or mixtures
4. Production, processing and distribution of food		▪ Food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council(3)which are engaged in wholesale distribution and industrial production and processing

Sectors overview - OTHER CRITICAL SECTORS

Sector	Subsector	Type of entity
5. Manufacturing	(a) Manufacture of medical devices and in vitro diagnostic medical devices	▪ Entities manufacturing medical devices as defined in Article 2, point (1), of Regulation (EU) 2017/745 of the European Parliament and of the Council(4), and entities manufacturing in vitro diagnostic medical devices as defined in Article 2, point (2), of Regulation (EU) 2017/746 of the European Parliament and of the Council(5)with the exception of entities manufacturing medical devices referred to in Annex I, point 5, fifth indent, of this Directive
	(b) Manufacture of computer, electronic and optical products	▪ Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2
	(c) Manufacture of electrical equipment	▪ Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2
	(d) Manufacture of machinery and equipment n.e.c.	▪ Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2
	(e) Manufacture of motor vehicles, trailers and semi-trailers	▪ Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2
	(f) Manufacture of other transport equipment	▪ Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2
6. Digital providers		▪ Providers of online marketplaces ▪ Providers of online search engines ▪ Providers of social networking services platforms
7. Research		▪ Research organisations