.

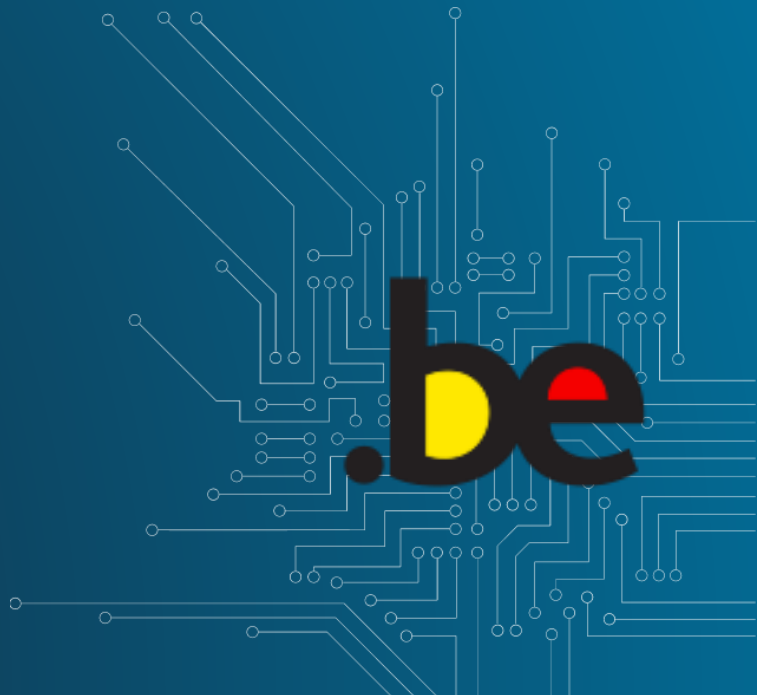
CENTRE FOR CYBER SECURITY BELGIUM

CERT.be The Federal Cyber Emergency Team

ibz Centre de crise Intérieur

06/2019

Implementation in Belgium of the "NIS" Directive (EU 2016/1148) of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union



Law of April 7th 2019 establishing a framework for the security of networks and information systems of general interest for public security (*Official publication, M.B./B.S.,* May 3rd 2019)

Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (en abrégé « loi NIS ») :

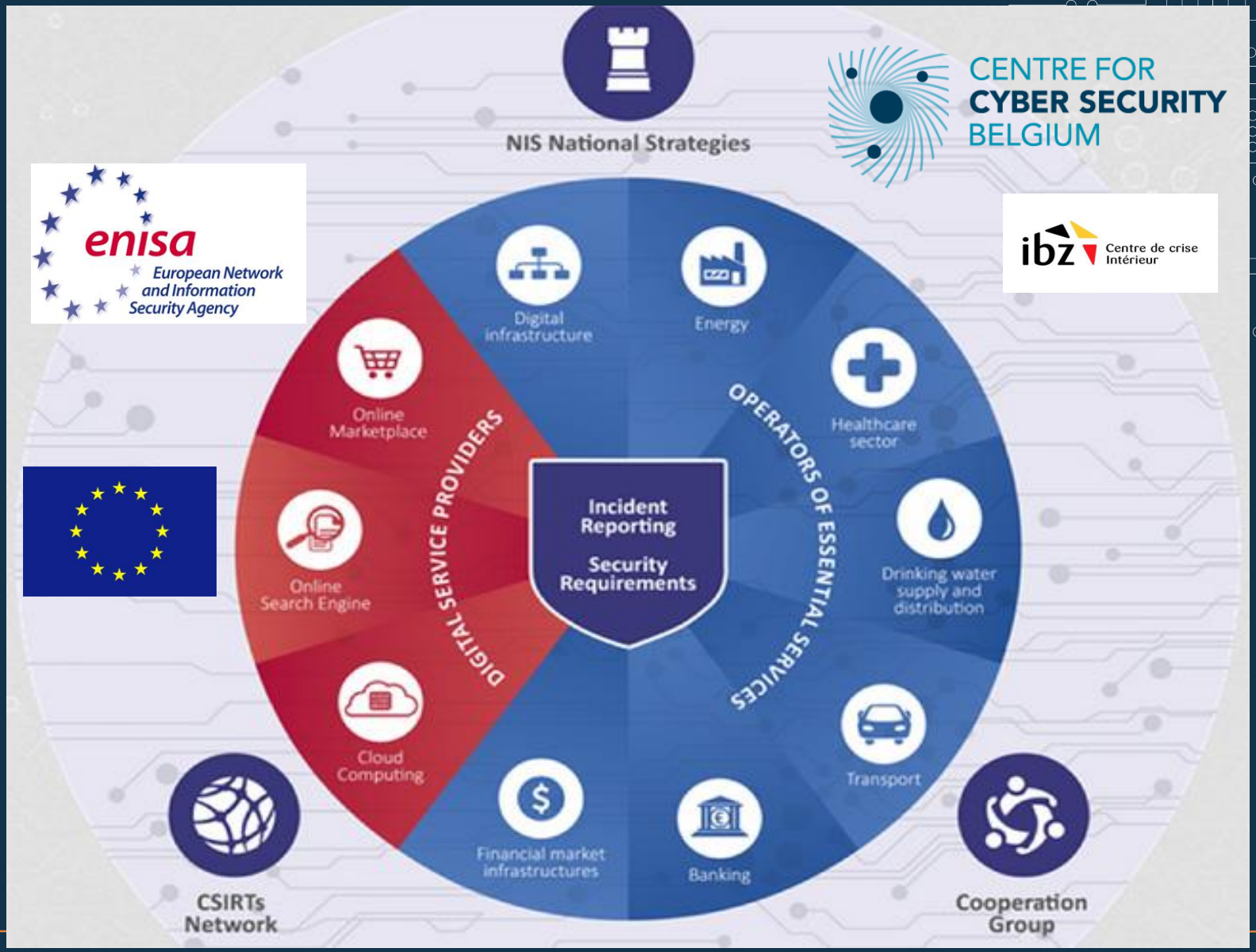
www.ejustice.just.fgov.be/cgi/article.pl?numac=2019011507&caller=list&article_lang=F&pub_date=2019-05-03&language=fr

Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (in afkorting "NIS wet") :

www.ejustice.just.fgov.be/cgi/article.pl?numac=2019011507&caller=list&article_lang=N&row_id=1&pub_date=2019-05-03&language=nl

Roles of the national authority (CCB), the DGCC and the sectoral authorities

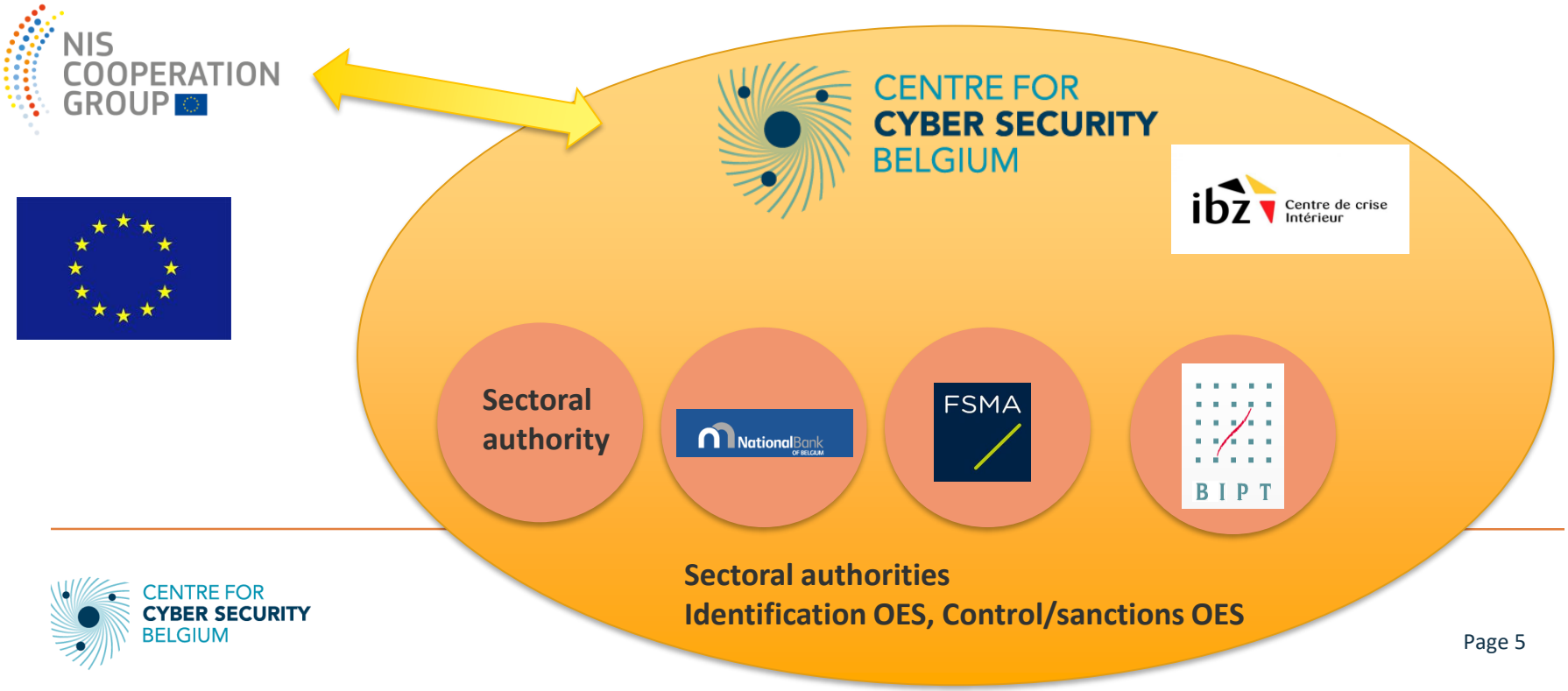
CENTRE FOR
CYBER SECURITY
BELGIUM


NIS National Strategies
CENTRE FOR CYBER SECURITY BELGIUM
enisa
European Network and Information Security Agency
ibz
Centre de crise
Intérieur
Digital infrastructure
Energy
Healthcare sector
Drinking water supply and distribution
Transport
Banking
Financial market infrastructures
Cloud Computing
Online Search Engine
Online Marketplace
DIGITAL SERVICE PROVIDERS
OPERATORS OF ESSENTIAL SERVICES
Incident Reporting
Security Requirements
CSIRTs Network
Cooperation Group

1. Centre for Cybersecurity Belgium (CCB): national coordination authority, EU SPOC (EU NIS Cooperation Group), national CSIRT (EU NIS CSIRT network), NIS national strategy coordinator

2. Direction General Crisis Centre (DGCC) of the FPS Interior: support for the identification of OES and the incident notification (crisis management)

3. Sectoral authorities: BNB, FSMA, BIPT (Digital infrastructures), FPS Mobility, FPS Economy (DG Energy & DSP), FPS Public health (Healthcare), National Security authority for supply and distribution of drinking water (to be created)



Designation of sectoral authorities (law of 7.04.2019 or Royal decree xx.07.2019)

1. Energy (Electricity, Gas, Oil): federal Energy Minister (Federal Public Service – FPS Economy DG Energy);

2. Transport (Air transport, Rail transport, Water transport, Road transport): federal Mobility Minister (Federal Public Service - FPS Mobility and Transport);

Except transport by water transport accessible to sea vessels: the Federal Maritime Mobility Minister

4. Health sector: federal Health Minister (Federal Public Service - FPS Public Health);

5. Digital Infrastructure: Belgian Institute for Postal services and Telecommunications (BIPT)

6. Drinking water supply and distribution: National authority for the security of drinking water supply and distribution (to be created with representatives of the Regions)

Financial sector (*Lex specialis – applying EU specific regulations*)

National Bank of Belgium (BNB/NBB)

- Credit institutions
- Central counterparties
- Financial institutions (other than credit institutions and central counterparties) subject to the supervision of the National Bank of Belgium pursuant to Articles 8 and 12a of the Law of 22 February 1998 on the organic status of the National Bank of Belgium

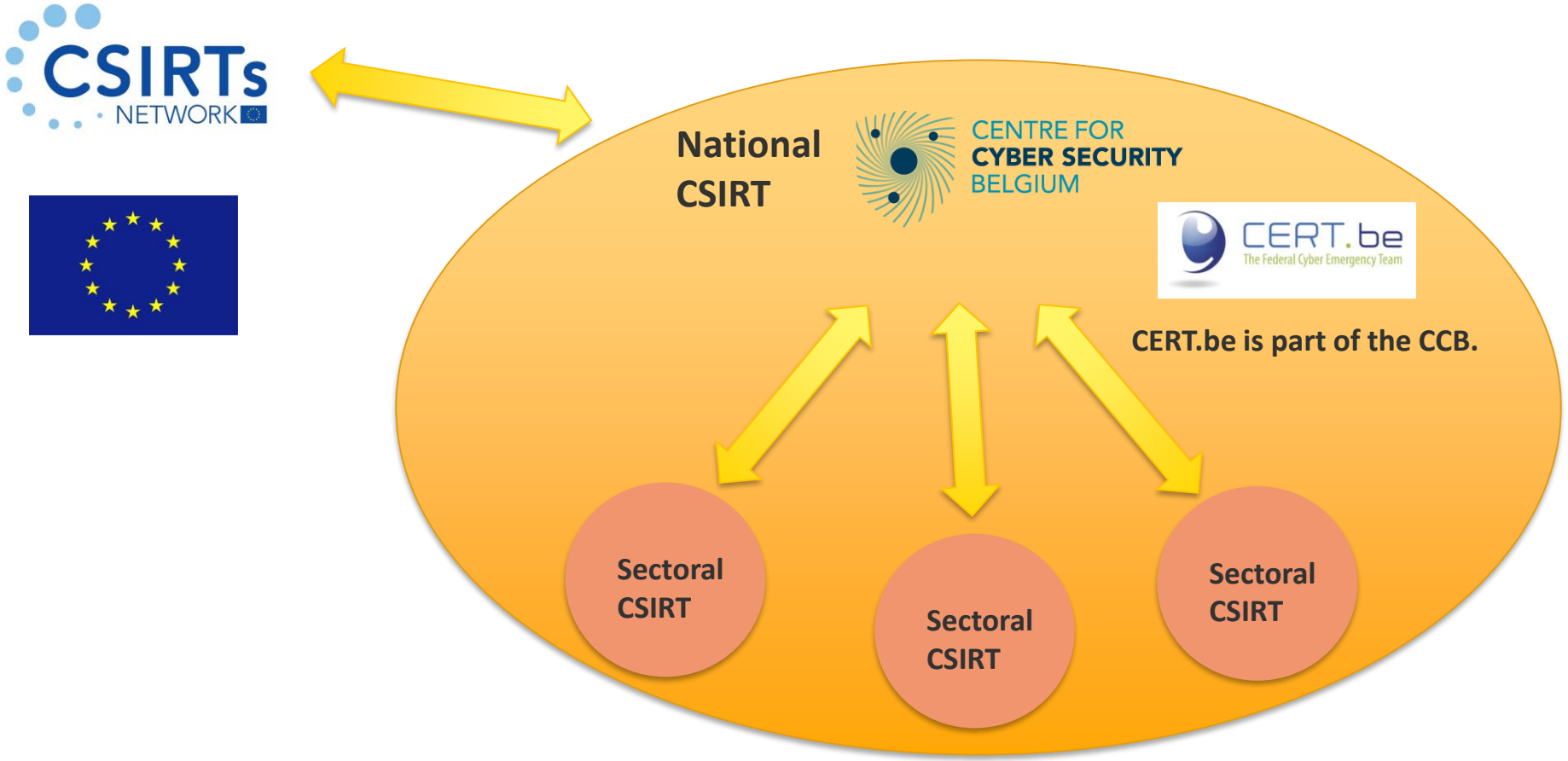
FSMA (Financial Services and Markets Authority)

- Operators of trading venues

;

National CSIRT: CCB (coordination for all sectoral) – service CERT.be

+ possible sectoral CSIRTs (to support the national CSIRT)



Tasks of the national CSIRT (CCB)

Tasks of the national CSIRT shall include at least the following:
(a) **monitoring incidents at national and international level**, including the processing of personal data relating to the monitoring of these incidents;
(b) **provide early warnings, alerts, announcements and dissemination of information** on risks and incidents to relevant stakeholders;
(c) **respond to incidents**;
(d) **provide a dynamic risk and incident analysis** and situation knowledge;
(e) **detect, observe and analyse computer security problems**;
(f) to encourage the identification and **use of common or standardized practices** in the field of procedures for the treatment of incidents and risks, and systems for the classification of incidents, risks and information;
(g) **ensure cooperation-oriented contacts** with the private sector and with other administrative services or public authorities;
(h) **participate in the EU CSIRT network** referred to in Article 12 of the NIS Directive;

Tasks of the national CSIRT (CCB)

In the exercise of its powers, the **national CSIRT shall take all appropriate measures to achieve its missions**.

These **measures must be proportionate to those objectives and in accordance with the principles of objectivity, transparency and non-discrimination**.

In achieving those objectives, the national CSIRT **may retain all available data, disclose it to another person or distribute it, or make use of it, even that data resulting from unauthorized access to a computer system by a third party**.

The national CSIRT fulfills its tasks with the necessary caution that may be expected from a government. Priority must always be given to ensuring that the operation of the computer system is not disrupted and that all reasonable precautions must be taken to prevent material damage to the IT system.

Tasks of the sectoral CSIRT

Tasks of a sectoral CSIRT shall, in cooperation with the national CSIRT, include at least the following:
(a) monitoring sectoral incidents;
(b) provide early warnings, alerts, announcements and dissemination of information on risks and incidents to relevant stakeholders in the sector;
(c) respond to sectoral incidents;
(d) ensure dynamic analysis of risks of sectoral incidents and situational knowledge;
(e) ensure cooperation-oriented contacts with the suppliers of its sector;
(f) be able to participate in meetings of the CSIRT network referred to in Article 12 of the NIS Directive, which are dedicated to its sector.

Operators of essential services (“OES”) in Belgium

operator having at least one establishment on the Belgian territory and actually carrying out an activity related to the provision of at least one essential service in the Belgium.

CENTRE FOR
CYBER SECURITY
BELGIUM

Identification of operators of essential services by the sectoral authority for each sector

The general criteria for the identification of the operators of essential services :

(a) an entity provides **a service which is essential for the maintenance of critical societal and/or economic activities**;

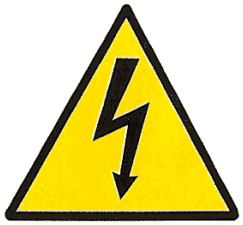
(b) the provision of that **service depends on network and information systems**; and

(c) an incident would have **significant disruptive effects on the provision of that service**.

Specific criteria/thresholds to be defined by sectoral authorities (in coordination with CCB and DGCC)




Annex II of the NIS directive (EU 2016/1148 July 6th 2016)



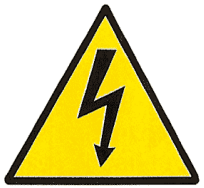
Energy

Electricity
- Electricity undertakings
- Distribution system operators
- Transmission system operators

Oil
- Operators of oil transmission pipelines
- Operators of oil production, refining and treatment facilities, storage and transmission

Gas
- Supply undertakings
- Distribution system operators
- Transmission system operators
- Storage system operators
- LNG system operators
- Natural gas undertakings
- Operators of natural gas refining and treatment facilities

Annex I of the law of April 7th 2019



Types of operators of essential services referred to in Article 11(1) of the law

1. Energy	**a) Electricity**	**Electricity companies within the meaning of Article 2, 15 ° ter of the Act of 29 April 1999 on the organization of the electricity market.**
		Distribution system operators within the meaning of Article 2, 11 ° of the Act of 29 April 1999 on the organization of the electricity market.
		Grid operators within the meaning of Article 2, 8 ° of the Act of 29 April 1999 on the organization of the electricity market.

economie
FPS Economy, S.M.E.s, Self-employed and Energy

Annex I of the law of 7.04.2019

Types of operators of essential services referred to in Article 11(1)

	b) Petroleum	**Oil pipeline operators.**
		Operators of installations for the production, refining, processing, storage and transport of petroleum.

economie
FPS Economy, S.M.E.s, Self-employed and Energy

Annex I of the law of 7.04.2019

Types of operators of essential services referred to in Article 11(1)

	c) Gas	**Natural gas undertakings within the meaning of Article 1, 5 ° bis of the Law of 12 April 1965 on the transport of gaseous products and others by piping.**
		Distribution system operators within the meaning of Article 1, 13 ° of the Law of 12 April 1965 on the transport of gaseous products and others by means of pipelines.
		Managers of the natural gas transmission network within the meaning of Article 1, 31 ° of the Law of 12 April 1965 on the transport of gaseous products and others by means of pipes.
		Storage managers in the sense of article 1, 33 °, of the law of 12 April 1965 concerning the transport of gaseous products and others by means of pipes.
		Managers of the LNG installation within the meaning of article 1, 35 °, of the law of 12 April 1965 concerning the transport of gaseous products and others by means of pipes.
		Operators of natural gas refining and processing plants.

economie
FPS Economy, S.M.E.s, Self-employed and Energy

Annex II of the NIS directive (EU 2016/1148 July 6th 2016)

Transport

Air transport

- Air carriers
- Airport managing bodies
- Traffic management control operators providing air traffic control (ATC) services

Rail transport

- Infrastructure managers
- Railway undertakings

Water transport

- Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport
- Managing bodies of ports
- Operators of vessel traffic services

Road transport

- Road authorities
- Operators of Intelligent Transport Systems

Transport

Federal Public Service
Mobility and Transport

2. Transport	**a) Air transport**	**Air carriers within the meaning of Article 3 (4) of Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.**
		Airport operators within the meaning of Article 2 (2) of the Royal Decree of 6 November 2010 on access to the ground handling market at Brussels National Airport, airports within the meaning of Article 2 (1) of Directive 2009/12/EC of the European Parliament and of the Council, including the airports belonging to the core network listed in Annex II Section 2 of Regulation (EU) No 1315/2013 of the European Parliament and of the Council, as well as entities operate associated installations located at airports.
		Air navigation services within the meaning of Article 2 (4) of Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the Single European Sky ("the framework regulation").
		The network manager within the meaning of Article 2 (22) of Commission Regulation (EU) No 677/2011 of 7 July 2011 laying down detailed rules for the implementation of air traffic management network functions and amending Regulation (EU) No 691/2010.

Transport

Federal Public Service
Mobility and Transport

	b) Rail transport	**Infrastructure managers** within the meaning of Article 3, 29 ° of the Rail Codex.
		Railway undertakings within the meaning of Article 3, 27 ° of the Rail Codex.

Transport

Federal Public Service
Mobility and Transport

	c) Transport over water	**Businesses for land, sea and coastal transport of passengers and goods** within the meaning of Annex I of Regulation (EC) No 725/2004 of the European Parliament and of the Council, except vessels operated individually by those companies.
		Administrators of ports within the meaning of Article 5 (7) of the Act of 5 February 2007 on maritime security, including their port facilities within the meaning of Article 2 (11) of Regulation (EC) No 725/2004, as well as entities that manage work and equipment in ports.
		Traffic Control Systems Operators within the meaning of Article 1 (12) of the Royal Decree of 17 September 2005 transposing Directive 2002/59/EC of 27 June 2002.

Transport

Federal Public Service
Mobility and Transport

	d) Road transport	**Road authorities** within the meaning of Article 2 (12) of Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council as regards the granting of EU -wide real-time traffic information services, responsible for traffic management control.
		Operators of intelligent transport systems within the meaning of Article 3 (1) of the Law of 17 August 2013 creating the framework for the introduction of intelligent transport systems and amending the Law of 10 April 1990 regulating private and special safety (quoted as "ITS framework law").

Annex II of the NIS directive (EU 2016/1148 July 6th 2016)

Finances

Credit institutions
Operators of trading venues
Central counterparties
Financial institutions (other than credit institutions and central counterparties) subject to the supervision of the National Bank of Belgium pursuant to Articles 8 and 12a of the Law of 22 February 1998 on the organic status of the National Bank of Belgium

Health sector

Health care settings (including hospitals and private clinics)
Healthcare providers

Drinking water supply and distribution

Suppliers and distributors of water intended for human consumption

Digital Infrastructure

IXPs
DNS service providers
TLD name registries

3. Finances	**a) Financial institutions**	**Credit institutions within the meaning of Article 4 (1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.**
		Central counterparties within the meaning of Article 2 (1) of the Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories.
		Financial institutions (other than credit institutions and central counterparties) subject to supervision by the National Bank of Belgium pursuant to Articles 8 and 12bis of the Act of 22 February 1998 establishing the Organic Statute of the National Bank of Belgium.

	b) Financial trading platforms	**Operators of a trading platform within the meaning of Article 3, 6 ° of the Act of 21 November 2017 on infrastructures for the markets for financial instruments and implementing Directive 2014/65/EU.**

federal public service
HEALTH, FOOD CHAIN SAFETY AND ENVIRONMENT

4. Healthcare	**Healthcare institutions (including hospitals and private clinics)**	**Caregivers within the meaning of Article 3 point (g) of Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare.**

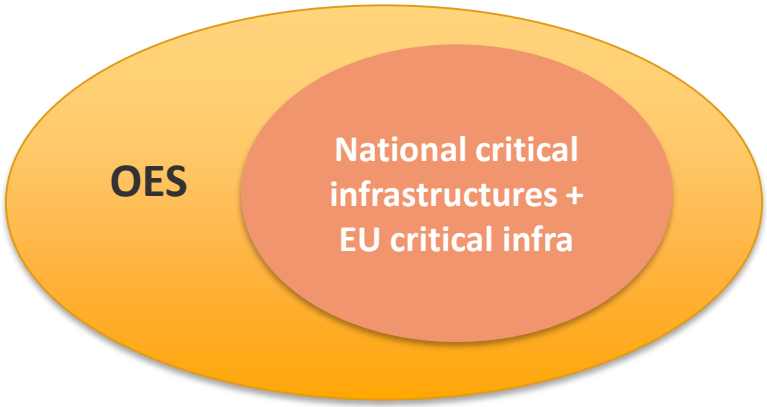
5. Drinking water		**Suppliers and distributors of water intended for human consumption within the meaning of Article 2 (1) (a) of Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption, except distributors for whom the distribution of water intended for human consumption is only a part of their general distribution activity of other products and goods that are not regarded as essential services.**

6. Digital infrastructures		**IXP.**
		DNS service provider.
		Top-level domain names registry.

Relation between operators of essential services (law of 7.04.2019) and critical infrastructures (law of 11.07.2011)

CENTRE FOR CYBER SECURITY BELGIUM

ibz Centre de crise Intérieur



identified operator of critical infrastructures (CI) => OES

Security requirements

CENTRE FOR
CYBER SECURITY
BELGIUM

Primary legislation (law of 7.04.2019) : General security obligation on OES --> adoption of a PSI (security policy for information systems and networks)
Chapter 2: Security measures

Art. 20.
The operator of essential services **shall take the necessary and proportionate technical and organisational measures to manage the risks that threaten the security of the networks and information systems on which its essential services depend.**

These measures shall ensure, for networks and information systems, a level of physical and logical security appropriate to the existing risks, taking into account the state of knowledge.

The operator shall also take appropriate measures to prevent or limit the impact of incidents that compromise the security of the networks and information systems used to provide these essential services, with a view to ensuring the continuity of these services.

Art. 21.
1. The essential services operator shall draw up a security policy for its information systems and networks (hereinafter referred to as "P.S.I.") setting out at least the objectives and practical security measures referred to in Article 20.

2. The essential services operator shall prepare its ISP at the latest within 12 months of notification of its designation. Within 24 months at the latest from the notification of its designation, it shall implement the measures provided for in its I.S.P.
For a given sector or, where appropriate, by sub-sector, the competent sectoral authority may adjust this period according to the type of measures provided for in the PSI.

Own risk analysis (own security policy) // GDPR

OES takes **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 risk posed**.

OES takes **appropriate measures to prevent and minimise the impact of incidents** affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

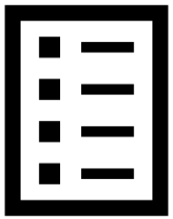
Accountability of the OES to prove its conformity with the security requirements general obligations

Are the technical and organisational security measures of network and information systems used for providing essential services appropriate and proportionate ?

Art. 23. 1. The essential services operator shall **designate its contact point for the security of information systems and networks** and shall communicate the data to the competent sectoral authority within three months of notification of designation as an essential services operator and, without delay, after each update of such data.
The sectoral authority shall make these data available to the authorities referred to in Article 7(1) and (4).

2. Where a safety contact point already exists under national or international provisions applicable in a sector or subsector, the essential services operator shall communicate its contact details to the sectoral authority within the time limits referred to in paragraph 1.

3. the contact point for the security of information systems and networks referred to in paragraph 1 shall be available at any time.



Secondary legislation (by Royal Decree) : <u>mandatory specific security requirements</u> for OES in one or more sectors

Art. 21
3. After consulting the authorities referred to in Article 7 and, where appropriate, after consulting the regions or communities concerned, **the King may impose certain safety measures applicable to operators of essential services in one or more sectors.**

Administrative acts (sectoral authority decisions): <u>individual additional mandatory security requirements</u>

Art. 21
4. **The sectoral authority**, in consultation with the authority referred to in Article 7(1) and, where appropriate, after consultation with the regions or communities, may, by **individual administrative decision, impose additional security measures**.

Primary legislation (Law)/ Guidance : **presumption of the security requirements conformity with a ISO/IEC 27001 certificate (issued by a conformity assessment body accredited)**

Art. 22. 1. The ISP referred to in Article 21(1) shall, in the absence of proof to the contrary, be presumed to comply with the safety requirements referred to in Article 20, when the safety measures it contains comply with the requirements of ISO/IEC 27001 or with a national, foreign or international standard recognised as equivalent by the King, by decree deliberated by the Council of Ministers.
The order referred to in paragraph 1 shall be issued after consultation with the national accreditation authority, the sectoral authority and the authority referred to in Article 7(1).

2. Compliance with the requirements referred to in paragraph 1 shall be established by a certificate issued by a conformity assessment body accredited according to ISO/IEC 17021 or ISO/IEC 17065 by the national accreditation authority or by an institution which is a co-signatory to the recognition agreements of the European Cooperation for Accreditation.
The certificate issued must fall within the scope of the certification for which the conformity assessment body has been accredited and cover the entire content of the ISP.

Recommendation certification ISO 27001 of the NIS systems supporting the essential services - not mandatory

Conformity presumption of the information system and network security policy (ISP) with a **certification ISO 27001** (or recognized equivalent standards norms) delivered **by an organization accredited by BELAC** or by another EU accreditation recognized authority.

Unless proved otherwise, the OES can benefit of a presumption of conformity of the **content of its security policy (ISP) for networks and information systems** when its security measures meet the requirements of ISO / IEC 27001 (or a national, foreign or international standard **recognized as equivalent by Royal Decree**, after consultation with BELAC, the sectoral authority and the CCB).

Guidelines on the security requirements for OES

Reference document on security measures for Operators of Essential Services (CG Publication 01/2018)

ENISA Guidelines on assessing DSP security and OES compliance with the NISD security requirements

www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements

EU Minimum security requirements for Digital Service Providers (DSP)
Implementing Regulation of the European Commission of 30 January 2018 (EU) 2018/151
www.eur-lex.europa.eu/eli/reg_impl/2018/151/oj

ENISA Technical Guidelines for the implementation of minimum security measures for DSP
www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

Incident notification for OES

CENTRE FOR
CYBER SECURITY
BELGIUM

Art. 24. 1. The essential services operator shall notify, **without delay**, **all incidents having a significant impact** on the availability, confidentiality, integrity or authenticity of the networks and information systems on which the essential service or services it provides depend.

2. After consulting the national CSIRT [CCB], the authority referred to in Article 7(4) [DGCC], the sectoral authority and, where appropriate, the regions or communities concerned, the **King may establish impact levels and/or thresholds**, by sector or sub-sector, constituting at least a significant impact within the meaning of (1).

3. **In the absence of incidence levels and/or thresholds** referred to in paragraph 2, the operator **shall notify all incidents affecting the availability, confidentiality, integrity or authenticity of the networks and information systems on which the essential service or services it provides depend**.

4. The **King may create different categories of notification** depending on the degree of impact of the incident.

Art. 25. The notification referred to in Article 24 shall be made simultaneously to the national CSIRT, the sectoral authority or its sectoral CSIRT, and the authority referred to in Article 7(4).

The notification obligation applies even if the essential services operator **has only part of the relevant information to assess the significance of the impact of the incident**.

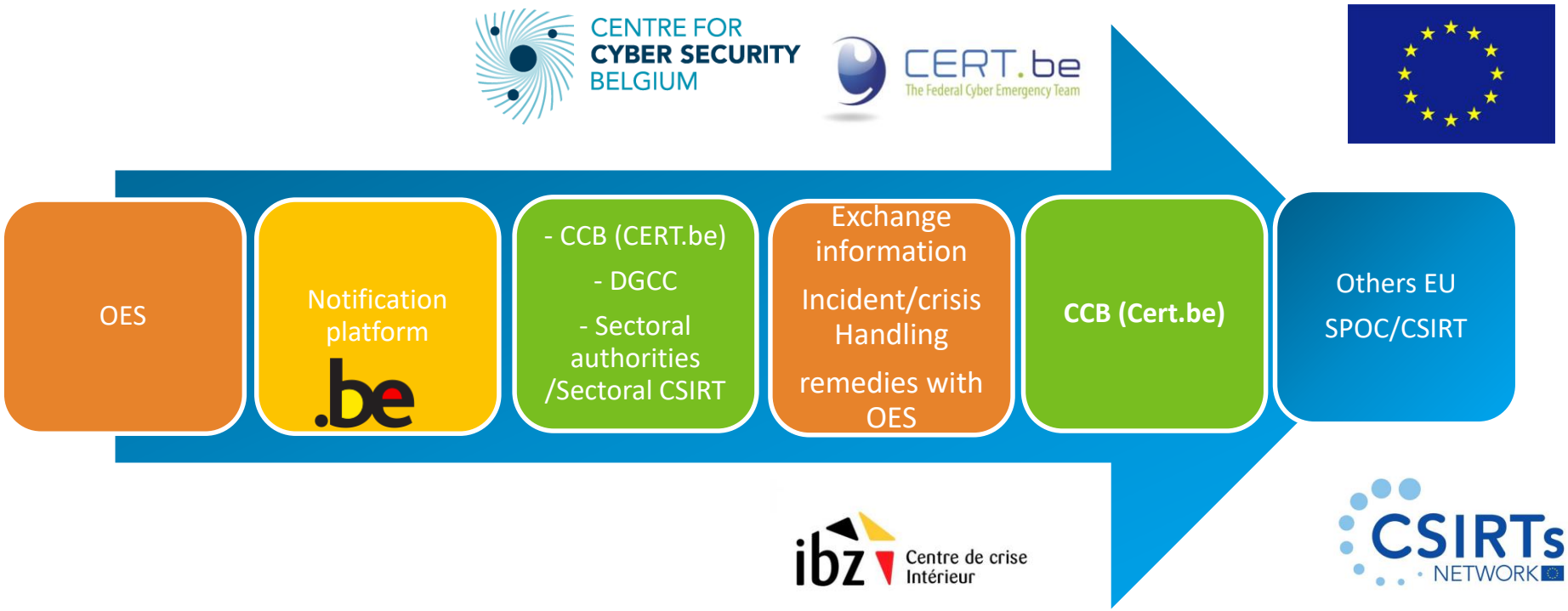
Art. 28. When an essential services operator is affected by an incident, the **OES must manage the incident and take reactive measures to resolve it**.

Incident management remains the responsibility of the OES.

The essential services operator shall **examine incidents or suspicious events** brought to its attention by the CCB, the sectoral authority or the DGCC.

Incident notification process for OES

Notification, without undue delay, of all incidents that have a significant impact on the availability, continuity, confidentiality, integrity or authenticity of the network and information systems of the OES providing an essential service.



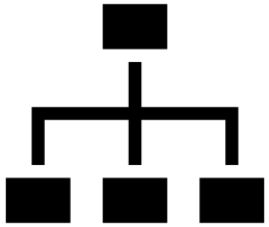
Incident notification process for OES under the supervision of the BNB

alignment with ECSB reporting requirements to financial regulators + critical infrastructures notification

Notification, without undue delay, of all incidents that have a significant impact on the availability, continuity, confidentiality, integrity or authenticity of the network and information systems of the OES providing an essential service.

PDF or Web form to use (tbc)

- **Mandatory notification → common notification platform**



Complete the webform www.nis-incident.be (not completely functional)

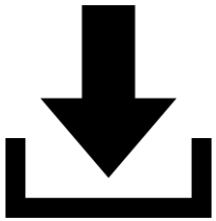
- **Voluntarity notification → notify the CCB (CERT.be)**

✓ **to use for mandatory notification while the common notification platform is not functional or available**

www.cert.be/en/report-incident

CENTRE FOR CYBER SECURITY BELGIUM

CERT.be The Federal Cyber Emergency Team



Notification : carried out via the notification platform and using the incident notification form determined by the national CSIRT (CCB – to be finalized).

The notification shall contain all available information to determine the nature, causes, effects and consequences of the incident.

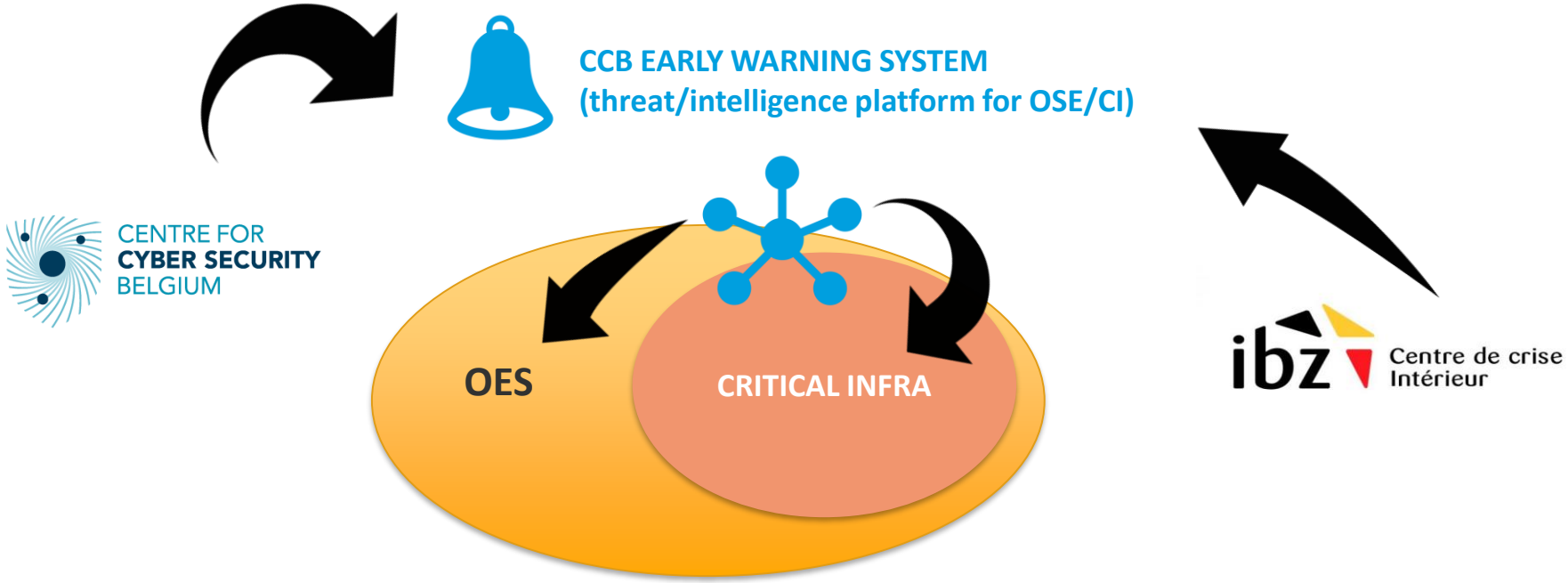
1° Initial notification

2° Additional notification (new information or developments become available)

3° Final report (at the request of the national CSIRT, DGGC, sectoral authority or its sectoral CSIRT)

NATIONAL VITAL SECTORS (public security)

Identified IC (law of 11.07.2011) => OES NIS (law of 7.04.2019)



Supervision - controls

CENTRE FOR
CYBER SECURITY
BELGIUM

Primary legislation (law of 7.04.2019) : controls on the OES

--> internal audit/every year(self-assessment)
--> external audit/every three years
--> inspection /any time

Chapter 1. Supervision of the operators of essential services
Section 1. Audits

Art. 38. 1. The operator of essential services carries out, on **an annual basis and at his expense**, **an internal audit of the network and information systems on which the essential services provided by him depend**. This internal audit must allow the operator of essential services to ensure that the measures and processes provided in his I.S.P. are properly applied and regularly monitored.

The operator of essential services provides the internal audit reports to the sectoral authority within thirty days.

2. The operator of essential services shall, **at least every three years and at his own expense, conduct an external audit by a conformity assessment body accredited** by the national accreditation authority or by an institution that has co-signed the recognition agreements of the "European Cooperation for Accreditation".
The operator of essential services provides the external audit reports to the sectoral authority within thirty days.

Secondary legislation (Royal Decree) : general accreditation conditions, audit rules**.**

Art. 39. 1. After obtaining advice from the sectoral authority and the authority referred to in Article 7(1), the King determines:
1° the **general accreditation** conditions based on the requirements of the ISO / IEC 17021 or ISO / IEC 17065 standards;
2° the **additional sectoral criteria** that the institution may be subject to for the conformity assessment;
3° the **rules that apply to the internal audit**;
4° the **rules that apply to the external audit**.

2. The King may by decree deliberated in the Council of Ministers, after advice from the sectoral authority and the authority referred to in Article 7, § 1, also determine the conditions for a possible recognition that is granted by the sectoral authority to a conformity assessment body.

3. The list of accredited or recognized conformity assessment bodies is available with the sectoral authority that keeps it up to date.
(…)

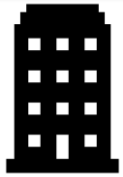
Section 2. Inspection services

Art. 42. 1. Inspection services can at any time carry out controls of the compliance with the security measures and the rules for reporting incidents by the operator of essential services.

2. The authority referred to in Article 7(1), or the sectoral authority may, provided that a justification is given, recommend the inspection service to carry out controls.

After advice from the sectoral authority and the authority referred to in Article 7(1), the King can determine possible sectoral practical modalities for the control.

Audits and controls of OES



Accreditation

OES
Internal audit
(1 x year)

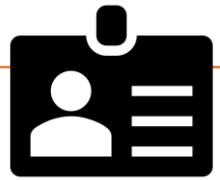
External auditors
(1 x 3 years) **accredited by BELAC or by sectoral authorities**

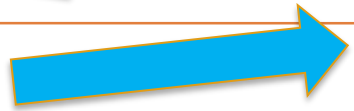
Sanctions *(criminal or administrative)*

Warning /Period to comply

Specific controls by **sectoral authorities (inspection services)**

Communication of the results of the external audits





CENTRE FOR CYBER SECURITY BELGIUM

CENTRE FOR CYBER SECURITY BELGIUM

Deadline for OES

12 months from the designation: OES shall **draft their security systems and information networks policy (P.S.I./I.B.B.)** (already developed for some operators in their "operator security plan" - critical infrastructures);

24 months from the designation: OES shall **implement the measures prescribed in its policy**

3 months after the of the elaboration of the P.S.I.: 1st internal security audit

24 months after the 1st internal audit: 1st external audit (carried out by an organization accredited by BELAC)

Sanctions



Art. 48. 1. When one or more breaches of the requirements of the law, their royal decrees or the related individual administrative decisions are identified, the inspection service **shall give a notice (warning)** to the operator of essential services or digital service provider in question to comply to its obligations within a term.
The term is determined taking into account the operating conditions of the operator of essential services or digital service provider and the measures to be taken.

Art. 49. 1. If the inspection service establishes that the operator of essential services or digital service provider does not comply with the notice of default within the set term, the facts shall be recorded in an official report by the sworn members of the inspection service. That official report is sent to the competent sectoral authority.
2. The fact that someone voluntarily obstructs or impedes the performance of an inspection by the members of the inspection service, refuses to communicate the information requested from him as a result of this inspection, or deliberately communicates incorrect or incomplete information, shall be recorded in an official report by the sworn members of the inspection service.
3. Paragraphs 1 and 2 also apply to the potential operator of essential services or to the operator of a critical infrastructure that does not comply with the information obligations referred to in Article 14 or Article 18(3).
4. The official reports drawn up by the sworn members of the inspection service shall have the value of evidence until proven otherwise.

Art. 50. Violations of the law or its implementing acts may give rise to **criminal or administrative sanctions**.

Criminal sanctions (by a criminal judge)

Art. 51. 1. Non-compliance with one of the notification obligations referred to in Article 24 or 36 shall be punishable by **imprisonment of eight days to one year** and a **fine of 26 euros to 20.000 €** or one of both penalties.

2. Non-compliance with one of the security obligations imposed by the King or the sectoral authority under Article 21 or 34 shall be punishable by **imprisonment of 8 days to 1 year** and a **fine of 26 € to 30.000 €** or one of both penalties.

3. Non-compliance with one of the **supervisory obligations** referred to in Chapters 1 and 2 of Title 4 shall be punishable by **imprisonment of 8 days to 1 year** and a **fine of 26 € to 50.000 €** or one of both penalties.

4. Non-compliance with one of **the information obligations** referred to in Article 14 or Article 18(3), shall be punishable by **imprisonment of 8 days to 1 year** and a **fine of 26 € to 50.000 €** or one of both penalties.

5. Any **voluntary obstruction or impediment to the performance of the inspection** by the members of the inspection service, refusal to communicate the information requested as a result of this inspection, or deliberate communication of incorrect or incomplete information shall be punished with imprisonment from **8 days to 2 years** and a **fine of 26 € to 75.000 €** or one of both penalties.

6. In case of repetition of the same facts within a period of three years, the fine will be **doubled** and the offender will be punished with a prison sentence of **15 days to 3 years**.

Administrative sanctions (by the sectoral authority)

Art. 52. 1. Any violation of this law, its implementing acts or the administrative decisions taken pursuant to this law may give rise to an administrative sanction.

2. **Failure to comply with the notification obligations** referred to in Article 24 or 36 shall be punishable by a fine of **500 € to € 75.000 €.**

3. **Non-compliance with the security obligations imposed by the King or the sectoral authority** pursuant to article 21 or 34 shall be punished by a fine of **500 to 100.000 €**.

4. **Non-compliance with the information obligations** referred to in Article 14 or Article 18(3), will be punished by a fine of **500 € to 125.000 €.**

5. **Non-compliance with the supervisory obligations** referred to in Chapters 1 and 2 of Title 4 will be punished by a fine of **500 € to 200.000 €**.

6. **Any act whereby a person acting on behalf of a operator of essential services or digital service provider suffers adverse consequences in the performance of the obligations arising from this law** in good faith and in the context of his duties, shall be punished with a fine of **500 € to 200.000 €**.

CENTER FOR CYBER SECURITY BELGIUM (CCB)
Federal administration under the authority of the Prime Minister
NIS Team
Rue de la Loi, 18
1000 Brussels

nis@ccb.belgium.be (legal and international relations dept.)
cert@cert.be (service CERT.be)

valery.vandergeeten@ccb.belgium.be

+32 (0)2 501 02 11 (legal and international relations dept.)
+32 (0)2 501 05 60 (service CERT.be)

www.ccb.belgium.be
www.cert.be
www.safeonweb.be

CENTRE FOR
CYBER SECURITY
BELGIUM

FEDERAL PUBLIC SERVICE HOME AFFAIRS
National Crisis Centre (NCCN)

Rue Ducale, 53
1000 Brussels

www.centredecrise.be/fr/contact
www.crisiscentrum.be/nl/contact

ibz Centre de crise Intérieur

CENTRE FOR CYBER SECURITY BELGIUM

FEDERAL PUBLIC SERVICE ECONOMY, S.M.E., SELF-EMPLOYED AND ENERGY
Bd du Roi Albert II, 16
1000 Brussels

info.eco@economie.fgov.be (contact center)
+32 0800 120 33 (contact center)

www.economie.fgov.be/nl/ons-contacteren
www.economie.fgov.be/fr/nous-contacter

For Operator of essential services in the Energy sector:

DG Energy
Division Nuclear Applications and Critical Infrastructures

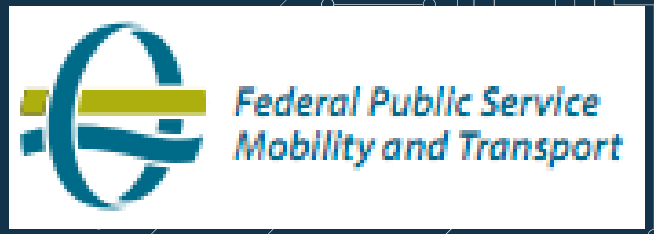
For Digital service providers :

DG Quality and Safety E 6
Division Metrology - Service Regulation Metrology

FEDERAL PUBLIC SERVICE MOBILITY AND TRANSPORT
Vooruitgangstraat, 56
1210 Brussels

info@mobilit.fgov.be
+32 2 277 31 11
www.mobilit.belgium.be

Alex DE SMET
Expert Coordinator
alex.desmet@mobilit.fgov.be
+32 2 277 39 91



FEDERAL PUBLIC SERVICE HEALTH, FOOD CHAIN SAFETY AND ENVIRONMENT
DG Healthcare
Place Victor Horta, 40 bte 10
1060 Brussels

Charles DENONNE
International relations
charles.denonne@health.fgov.be
02 524 97 37

Alain Quewet
Corporate Office
alain.quewet@health.fgov.be
02 524 70 85

Andries Nelissen
DG Soins de Santé
andries.nelissen@health.fgov.be
02 524 85 87

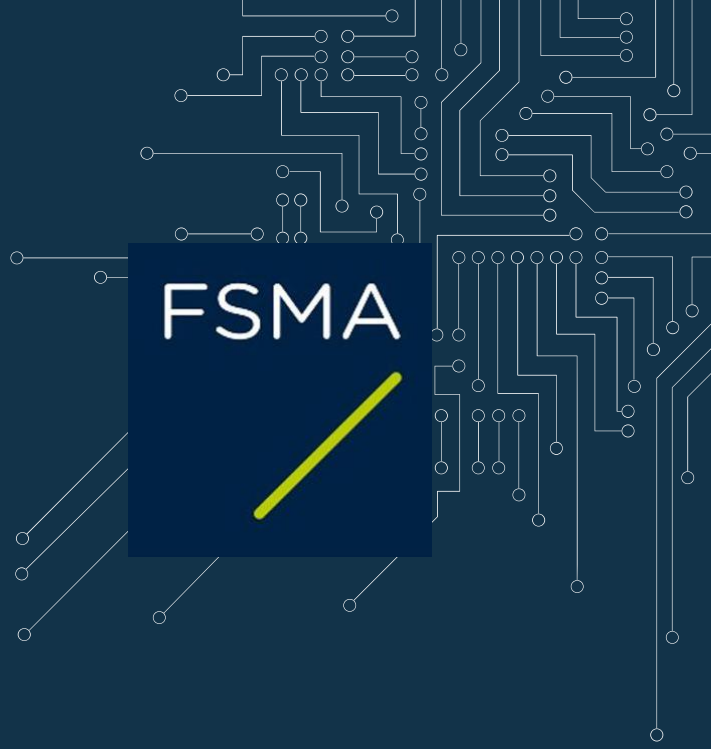
NATIONAL BANK OF BELGIUM
ORM – BCM Team
Boulevard de Berlaimont, 14
1000 Brussels
orm@nbb.be
spocvt@nbb.be

Mr Marc VERHELST
Operational risk management
+32 2 221 34 19
www.nbb.be

FINANCIAL SERVICES AND MARKETS AUTHORITY
Rue du Congrès, 12-14
1000 Brussels

Monsieur Antoine GREINDL
Legal Officer
Antoine.Greindl@fsma.be
+ 32 (2) 220 52 71

Monsieur Sébastien WOLFF
sebastien.wolff@fsma.be
+ 32 (2) 220 59 17



Belgian Institute for Postal services and Telecommunications
Network Security Dept.
Ellipse Building, Bâtiment C
Boulevard du Roi Albert II, 35
1030 Brussels

netsec@bipt.be

+ 32 (2) 226 88 88

www.bipt.be

National authority for the security of drinking water supply and distribution

(to be created with representatives of the Regions)

Digital services providers (DSP) in Belgium

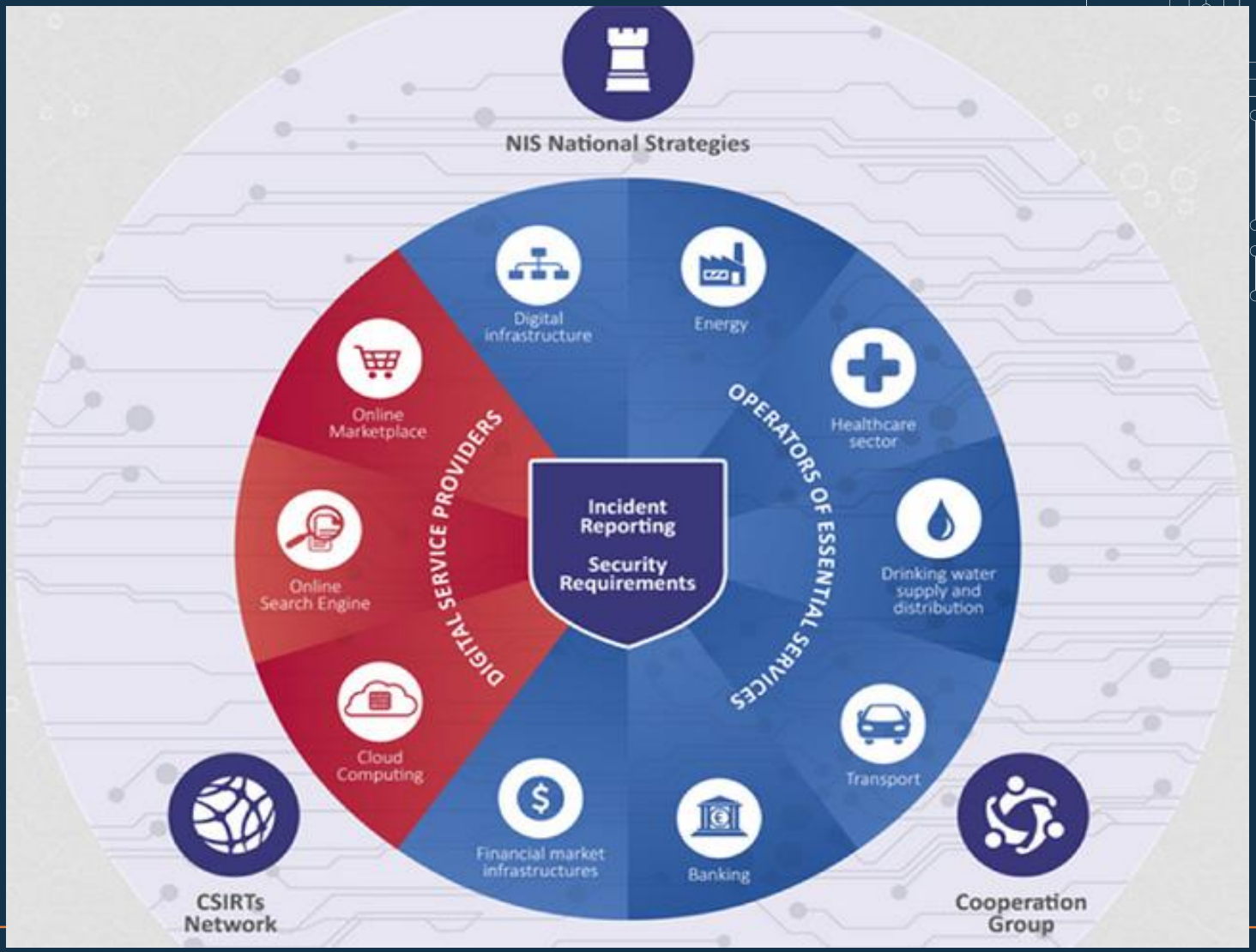
CENTRE FOR
CYBER SECURITY
BELGIUM

Annex II of the law of 7.04.2019

Types of digital services (Digital service providers)

1. Online marketplace
2. Online search engines
3. Cloud computing services

NIS directive



CENTRE FOR CYBER SECURITY BELGIUM

Digital service providers

- Three categories of digital service providers are defined in the Directive

- All entities meeting the definitions are automatically subject to the security and notification requirements under the NIS-Directive (no identification by the sectoral authority required).

1. Online marketplace ex: Ebay (not a e-shop of a company)

a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4 of Directive 2013/11/EU of the European Parliament and of the Council to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace

2. Online search engine

a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found,

3. Cloud computing service

a digital service that enables access to a scalable and elastic pool of shareable computing resources.

DSP outside the scope of the NIS Directive

- **Micro and small enterprises as defined in Commission Recommendation 2003/361/EC of 6 May 2003 are excluded from the scope of the Directive.**

DEFINITION OF MICRO, SMALL AND MEDIUM-SIZED ENTERPRISES

Article 1
Enterprise
An enterprise is considered to be any entity engaged in an economic activity, irrespective of its legal form. This includes, in particular, self-employed persons and family businesses engaged in craft or other activities, and partnerships or associations regularly engaged in an economic activity.

Article 2
Staff headcount and financial ceilings determining enterprise categories

1. The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.

2. Within the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons AND whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.

3. Within the SME category, a microenterprise is defined as an enterprise which employs fewer than 10 persons AND whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

National authorities for DSP (mix system: 1 national authority + 1 sectoral authority)

The national authorities cooperate closely in order to ensure compliance with the obligations of the NIS law.

Scope of the Belgian legislation

The Belgian law apply to digital service providers whose principal place of business (main establishment) is located in Belgium.

A digital service provider is deemed to have its principal place of business in Belgium when its registered office is located there.

A digital service provider that is not established in the European Union, but offers services referred in Annex III of the directive NIS within the Union, shall designate a representative in the Union (establishment of the representative in Belgium).

Security requirements and controls

A single set of EU rules applies

Implementing Regulation of the European Commission of 30 January 2018 (EU) 2018/151

laying down detailed rules for the application of Directive (EU) 2016 / 1148 which will apply for the rules to manage the risks that threaten the security of networks and information systems as well as the parameters to determine if an incident has a significant impact.

eur-lex.europa.eu/eli/reg_impl/2018/151/oj

enisa
European Network and Information Security Agency

Technical Guidelines for the implementation of minimum security measures for Digital Service Providers

www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

Rules to manage the risks that threaten the security of networks and information systems

Article 2. Security elements

1. Security of systems and facilities referred to in point (a) of Article 16(1) of Directive (EU) 2016/1148 means the security of network and information systems and of their physical environment and shall include the following elements:

(a) **the systematic management of network and information systems**, which means a mapping of information systems and the establishment of a set of appropriate policies on managing information security, **including risk analysis, human resources, security of operations, security architecture, secure data and system life cycle management and where applicable, encryption and its management**;

(b) **physical and environmental security**, which means the availability of a set of measures to protect the security of digital service providers' network and information systems from damage using an **all-hazards risk-based approach, addressing for instance system failure, human error, malicious action or natural phenomena**;

(c) **the security of supplies**, which means the **establishment and maintenance of appropriate policies in order to ensure the accessibility** and where applicable the **traceability of critical supplies** used in the provision of the services;

(d) **the access controls to network and information systems**, which means the availability of a set of measures to ensure that the **physical and logical access to network and information systems**, including administrative security of network and information systems, is authorised and restricted based on business and security requirements.

Article 2. Security elements

2. With regard to incident handling referred to in point (b) of Article 16(1) of Directive (EU) 2016/1148, the **measures** taken by the digital service provider shall include:

(a) detection processes and procedures maintained and tested to **ensure timely and adequate awareness of anomalous events**;
(b) processes and policies on **reporting incidents and identifying weaknesses and vulnerabilities** in their information systems;
(c) a **response in accordance with established procedures** and reporting the results of the measure taken;
(d) an **assessment of the incident's severity, documenting knowledge from incident analysis and collection of relevant information** which may serve as evidence and support a continuous improvement process.

3. **Business continuity management** referred to in point (c) of Article 16(1) of Directive (EU) 2016/1148 means the capability of an organisation to maintain or as appropriate restore the delivery of services at acceptable predefined levels following a disruptive incident and shall include:

(a) the establishment and the use of **contingency plans based on a business impact analysis** for ensuring the continuity of the services provided by digital service providers which shall be assessed and tested on a regular basis for example, through exercises;
(b) **disaster recovery capabilities** which shall be assessed and tested on a regular basis for example, through exercises.

Article 2. Security elements

4. **The monitoring, auditing and testing** referred to in point (d) of Article 16(1) of Directive (EU) 2016/1148 shall include the establishment and maintenance of policies on:

(a) the conducting of a planned sequence of **observations or measurements to assess whether network and information systems are operating as intended**;
(b) **inspection and verification** to check whether a standard or set of guidelines is being followed, records are accurate, and efficiency and effectiveness targets are being met;
(c) a **process intended to reveal flaws in the security mechanisms** of a network and information system that protect data and maintain functionality as intended. Such process shall include technical processes and personnel involved in the operation flow.

5. International standards referred to in point (e) of Article 16(1) of Directive (EU) 2016/1148 mean standards that are adopted by an international standardisation body as referred to in point (a) of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council. Pursuant to Article 19 of Directive (EU) 2016/1148, European or internationally accepted standards and specifications relevant to the security of network and information systems, including existing national standards, may also be used.

6. Digital service providers shall ensure that they **have adequate documentation** available to enable the competent authority to verify compliance with the security elements set out in paragraphs 1, 2, 3, 4 and 5.

Specific requirement in Belgium

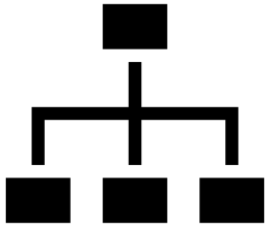
Digital service providers shall provide **a contact point for IT security and communicate the data to the FPS Economy**, as well as after each update of this data. The sectoral authority shall communicate this information to the national authorities (CCB, Crisis Centre, inspection service).

Incident notification process

Notification, without undue delay, any incident having a substantial impact on the provision of its digital service.

The notification shall be made simultaneously to the CCB (national CSIRT), the Federal Public Service Economy (sectoral authority) or its sectoral CSIRT and the Crisis Centre via the common notification platform.

- **Mandatory notification** → **common notification platform**



Complete the webform www.nis-incident.be (not completely functional)

- **Voluntarity notification** → **notify directly the CCB (CERT.be)**

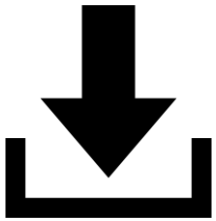
www.cert.be/en/report-incident

CENTRE FOR CYBER SECURITY BELGIUM

- ✓ **Also use for mandatory notification while the common notification platform is not functional or available**

www.cert.be/en/report-incident

CERT.be The Federal Cyber Emergency Team



Notification : carried out via the notification platform and using the incident notification form determined by the national CSIRT (CCB – to be finalized).

The notification shall contain all available information to determine the nature, causes, effects and consequences of the incident.

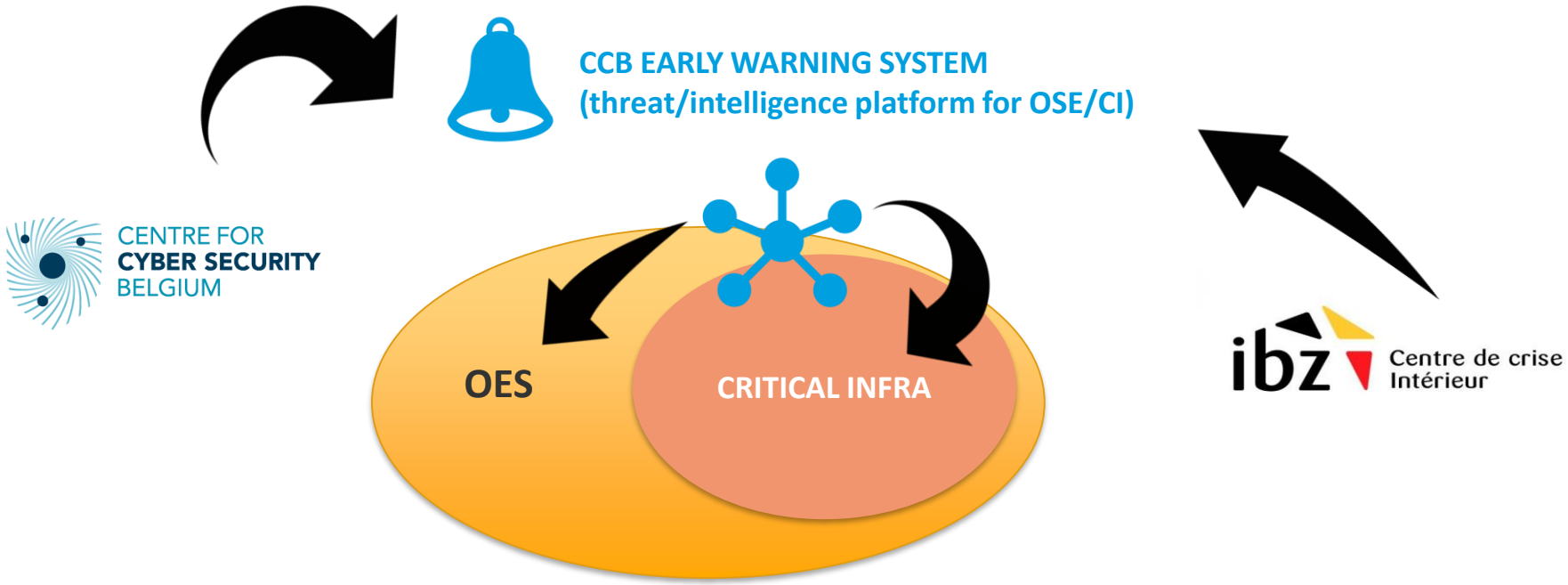
1° Initial notification

2° Additional notification (new information or developments become available)

3° Final report (at the request of the national CSIRT, DGGC, sectoral authority or its sectoral CSIRT)

NATIONAL VITAL SECTORS (public security)

Identified IC (law of 11.07.2011) => OES NIS (law of 7.04.2019)



Implementing Regulation of the European Commission of 30 January 2018 (EU) 2018/151

Parameters to determine if an incident has a substantial impact.

Article 3. Parameters to be taken into account to determine whether the impact of an incident is substantial

1. With regard to the number of users affected by an incident, in particular users relying on the service for the provision of their own services referred to in point (a) of Article 16(4) of Directive (EU) 2016/1148, **the digital service provider shall be in a position to estimate either of the following**:
(a) the number of affected natural and legal persons with whom a contract for the provision of the service has been concluded; or
(b) the number of affected users having used the service based in particular on previous traffic data.

2. The duration of an incident referred to in point (b) of Article 16(4) means the **time period from the disruption of the proper provision of the service in terms of availability, authenticity, integrity or confidentiality until the time of recovery**.

3. As far as the geographical spread with regard to the area affected by the incident referred to in point (c) of Article 16(4) of Directive (EU) 2016/1148 is concerned, the **digital service provider shall be in a position to identify whether the incident affects the provision of its services in specific Member States**.

4. The extent of disruption of the functioning of the service referred to in point (d) of Article 16(4) of Directive (EU) 2016/1148 shall be measured as regards one or more of the following characteristics impaired by an incident: **the availability, authenticity, integrity or confidentiality of data or related services**.

Parameters to determine if an incident has a substantial impact.

Article 4. Substantial impact of an incident

1. An incident shall be considered as having a substantial impact where at least one of the following situations has taken place:

(a) the service provided by a digital service provider was **unavailable for more than 5.000.000 user-hours** whereby the term user-hour refers to the number of **affected users in the Union for a duration of 60 minutes**;

(b) the incident has resulted in a **loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100.000 users in the Union**;

(c) the incident has created a **risk to public safety, public security or of loss of life**;

(d) the incident has caused **material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1.000.000**.

FEDERAL PUBLIC SERVICE ECONOMY, S.M.E., SELF-EMPLOYED AND ENERGY
Bd du Roi Albert II, 16
1000 Brussels

DG Quality and Safety E 6
Division Metrology - Service Regulation Metrology

Marc.Wouters_E6@economie.fgov.be

Mira.Fonteyne@economie.fgov.be
+32 (0) 22779365