



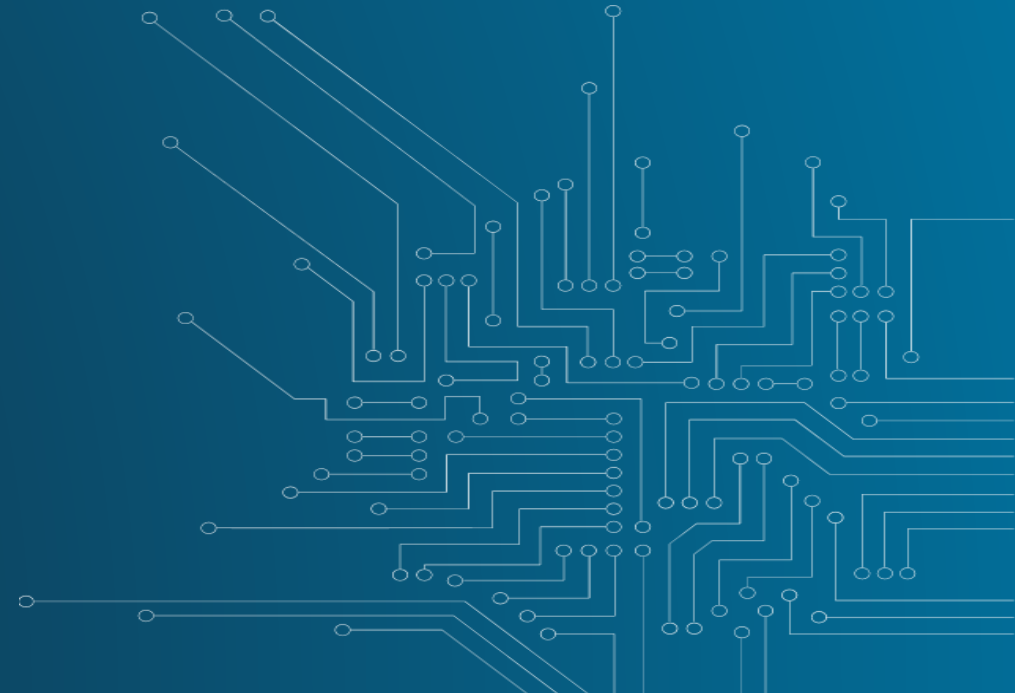
CENTRE FOR
CYBER SECURITY
BELGIUM

Manageable & effective NIS security measures

May, 11, 2022

NISDUC Workshop

Karl Dobbelaere (karl.dobbelaere@ccb.belgium.be)
Policy Manager, Centre for Cyber security Belgium (CCB)



Overview

- **NIS2 Scope**
 - Extra Sectors → diagram → 2 or 3 Categories
 - Registration (network & contact info, NIS-sector)
 - Tool
 - Criteria (interpretation) & Sanction
 - Identification: Vital, Crucial & Exception handling
- **Minimum Security Measures:**
 - Requirements
 - ENISA reference document on SecMeasures for OES + tool
 - Guidance doc
- **Supervision**
 - Self-assessment & Audit
 - ISP reporting
 - Inspection
- **Incident notification**

NIS 2 scope – Council position Annex I & II (March 2022)

Sector	Subsector	NIS-1 & CER entities (+ equivalent)	Large entities (more than 250 employees or more than 50 million revenue)	Medium (more than 50 employees or more than 10million revenue)	Small & Micro
Annex I					
1. Energy	Electricity; district Heating & cooling; Gas; Hydrogen; oil;	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, except if identified as essential or important by authorities due to sole service, significant impact, essential to society
2. Transport	Air; Rail; Water; Road				
3. Banking					
4. Financial Market Infrastructure					
5. Health					
6. Drinking Water					
7. Waste Water	(only if a main activity)	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, except if identified as essential or important by Member States due to sole service, significant impact, essential to society
8. Digital Infrastructure	TLD name registries				
	Qualified trust service providers				
	Non-qualified trust service providers				
	Providers of public electronic communications networks				
	DNS service providers				
	Internet Exchange Point providers				
	Cloud computing service providers				
	Data centre service providers				
	Content delivery network providers				
8a. ICT-service management	MSP, MSSP				
9. Public Administration entities	central governments (excluding administrations with any activity in judiciary, parliaments, central banks, defence, national security, public security or law enforcement)				
10. Space					

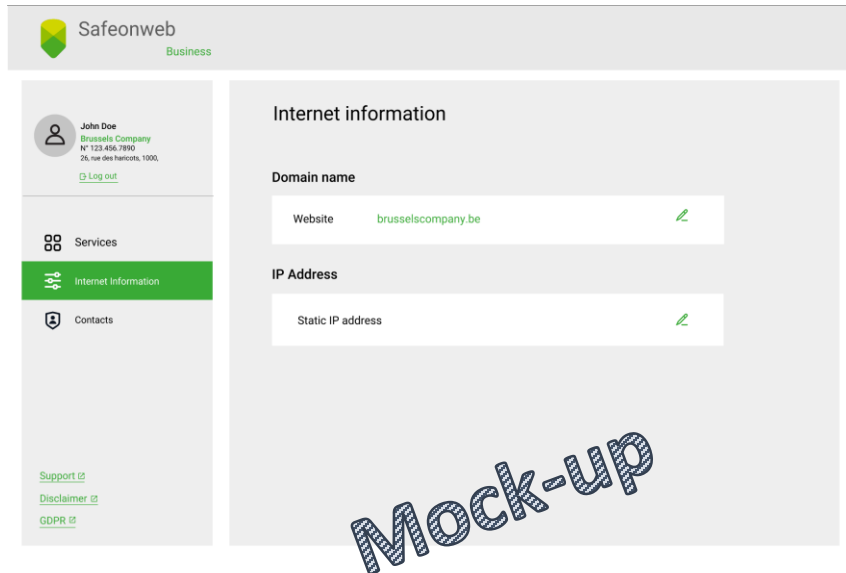
Annex II					
1. Postal and courier services		Essential	Important, except if identified as <u>essential</u> by sectoral authority	Important	Not in Scope, except if identified as <u>essential</u> or <u>important</u> by authorities due to sole service, significant impact, essential to society
2. Waste Management					
3. Chemicals					
4. Food					
5. Manufacturing					
6. Digital providers	online marketplaces, search engines, social networking				
Education and Research		Parliament Proposal			

- Additional sectors
- Additional entities (+2500)
- Identification as an exception process (for “upgrading”)

Challenges:

- Need for a registration mechanism?
- Need for a differentiated approach
 - Ensure continuity/compatibility with NIS1
 - Ability to handle steep volume increase
 - Risk management & Security measures
 - Incident reporting?
 - Supervision?
 - Sanctioning?
 - Inspection?

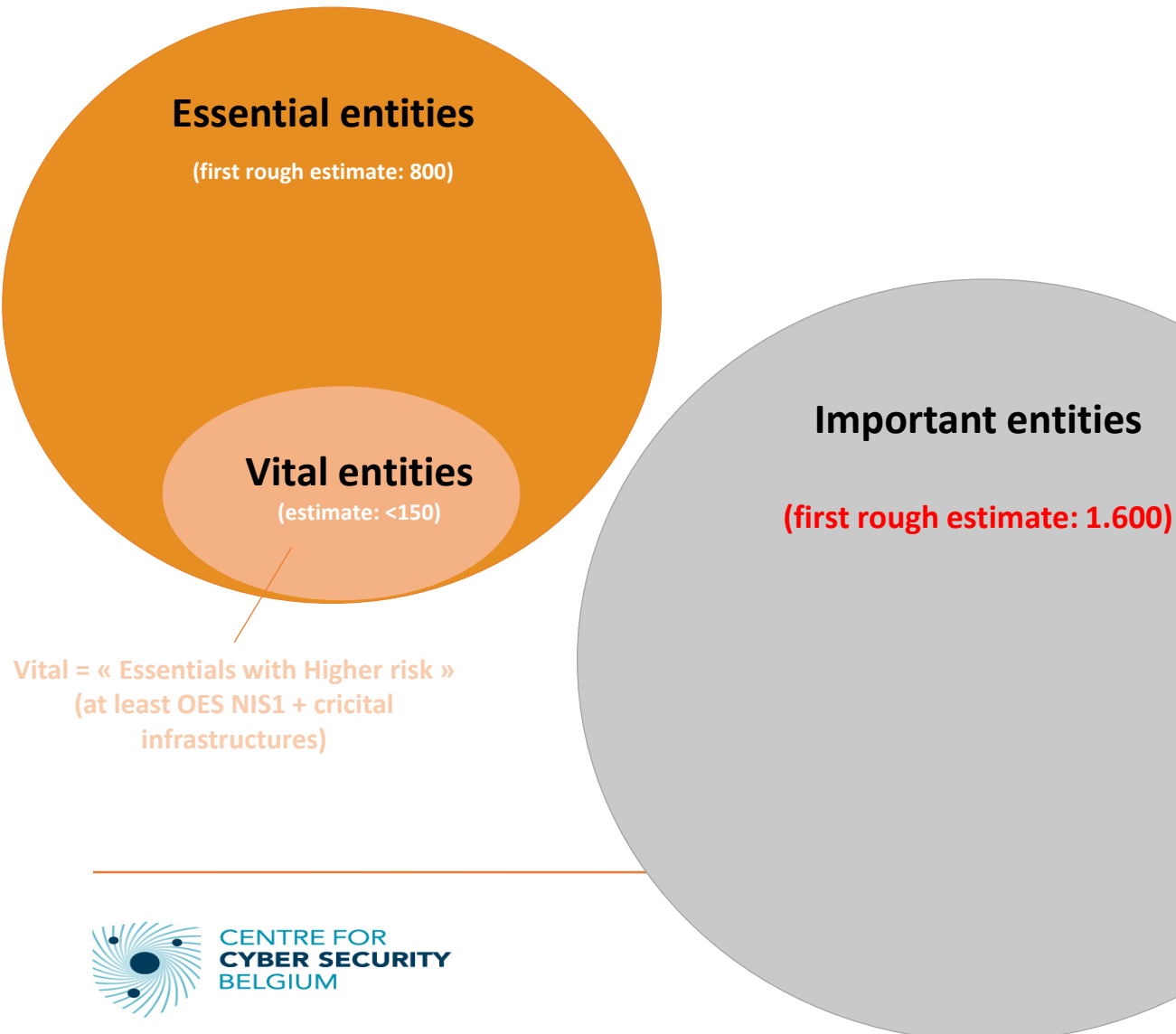
NIS 2 scope – Registration



The image shows a mock-up of the Safeonweb Business portal. The header includes the Safeonweb logo and 'Business' text. The left sidebar contains a user profile for 'John Doe' from 'Brussels Company', a 'Log out' link, and a menu with 'Services', 'Internet Information' (highlighted), and 'Contacts'. At the bottom of the sidebar are links for 'Support', 'Disclaimer', and 'GDPR'. The main content area is titled 'Internet information' and contains two sections: 'Domain name' with a 'Website' field containing 'brusselscompany.be', and 'IP Address' with a 'Static IP address' field. A large 'Mock-up' watermark is overlaid on the bottom right of the interface.

- With thousands of entities (currently <100), a **manual registration & onboarding** process is **no longer feasible**
- Need for digital transformation
- NIS entities will make use of CCB's portal for companies (Safeonweb4Business; currently under development) to
 - Register their contact & network data
 - Declare that they are a NIS-entity (possibly supported by means of a scope wizard)
 - Sign-up for additional Cybersecurity services
 - Cyber Threat Alert
 - Self-Assessment
 - Quick Scan Report

NIS 2 scope – Differentiation?



- With thousands of entities (i.o. <100), hard to apply a “one fits all” approach
- Need for differentiation:
 - Essential & Important as defined by NISD
 - Within Essentials: “Vitals”
 - NIS1 & CER entities
 - Extra through identification, risk-based (NIS2)
 - Continuation of current rules

NIS 2 scope – Security Measures: Principles

Focus on both Awareness & training, (Technical) Security Measures and Governance

ISO27001-equivalence mentioned in the NIS1-law might have lead to a misperception that governance aspects are considered more important than technical measures, training and awareness campaigns

Proportional requirements

Self-assessment, external audit and/or certification upon need

Minimize administrative burden

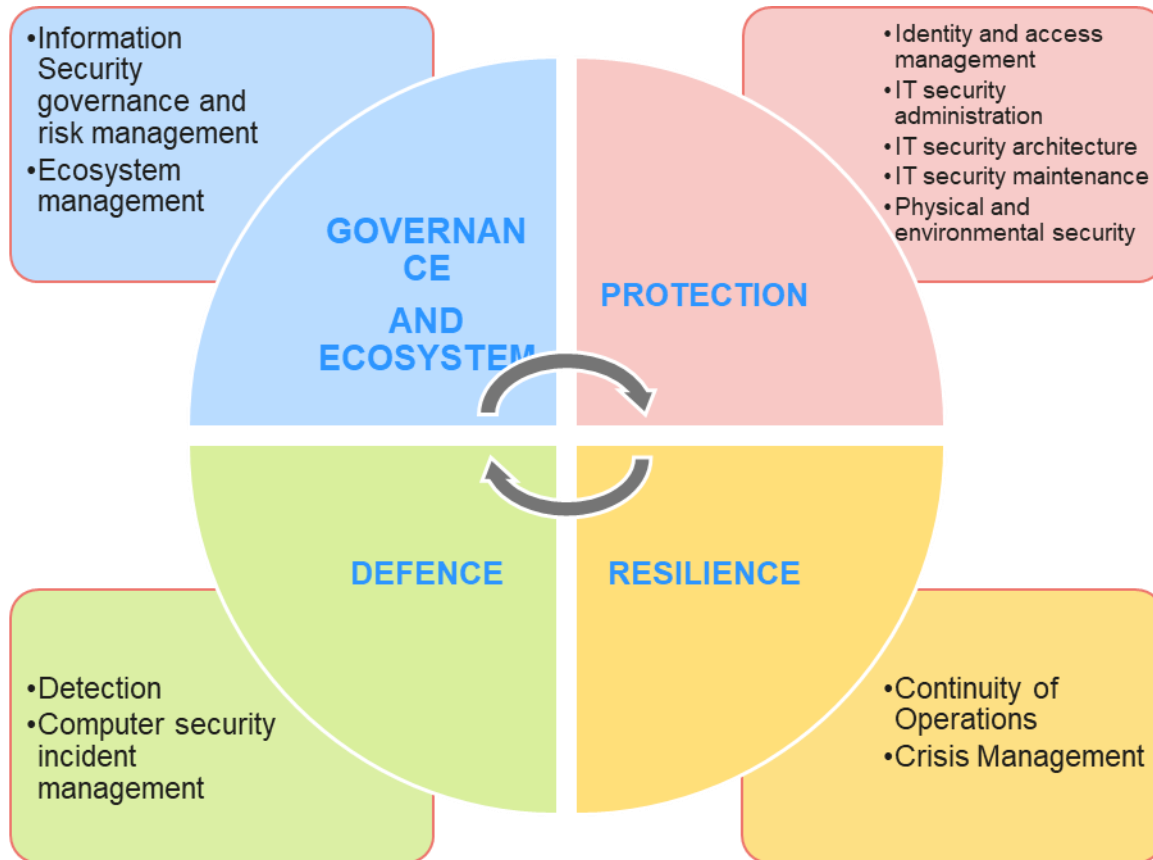
Multi-framework approach, transparant references

Compatibility with norms and frameworks already in use by the business community through mapping of the controls of common references (CIS, NIST, ISO...)

Continuity for NIS1 OES

The scope extension with NIS2 should not impact NIS1 OES

NIS 2 scope – Minimum Security Measures



ENISA : « *Minimum Security Measures for OES* » - [link](https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services)

Minimum Security Measures for OES

<https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services>

enisa

Search for resources, tools, publications and more

English (en)

TOPICS PUBLICATIONS TOOLS NEWS EVENTS ABOUT WORK WITH ENISA CONTACT

SECURITY MEASURES	ISO 27001	NIST CSF	ISA/IEC 62443
Incident Report	<ul style="list-style-type: none"> 7.5 Documented information A.12.1.1 Documented operating procedures A.16.1.1 Responsibilities and procedures A.16.1.2 Reporting information security events A.16.1.3 Reporting information security weaknesses 	<ul style="list-style-type: none"> RS.CO-2, 3, 4, 5 DE.DP-4 	<ul style="list-style-type: none"> SR.2.8 SR.2.9 SR.2.10 SR.2.11 SR.2.12 SR.3.9 SR.6.1 SR.6.2
Communication with competent authorities	<ul style="list-style-type: none"> 7.4 Communication 7.5 Documented information A.6.1.3 Contact with authorities A.6.1.4 Contact with special interest groups A.8.2.2 Labelling of information 	<ul style="list-style-type: none"> RS.CO-2, 3, 4, 5 DE.DP-4 	<ul style="list-style-type: none"> SR.2.8 SR.2.9 SR.2.10 SR.2.11 SR.2.12 SR.3.9 SR.6.1 SR.6.2
Logging	<ul style="list-style-type: none"> 9.1 Monitoring, measurement, analysis and evaluation A.12.4 Logging and monitoring A.14.1.2 Securing application services on public networks A.15.2.1 Monitoring and review of supplier services A.16.1.3 Protection of records 	<ul style="list-style-type: none"> ID.BA-1 ID.SC-1 PR.MA-1, 2 DE.CM-1, 2, 3, 6, 7 DE.AE-3 RS.MS-3 PR.PT-1 	<ul style="list-style-type: none"> SR.2.8 SR.2.9 SR.2.10 SR.2.11 SR.2.12 SR.3.9 SR.6.1 SR.6.2
Logs correlation and analysis	<ul style="list-style-type: none"> 9.1 Monitoring, measurement, analysis and evaluation 9.3 Management review A.16.1.4 Assessment of and decision on information security events 	<ul style="list-style-type: none"> ID.BA-4, 5 PR.PT-1 OP.AE-3, 4 	<ul style="list-style-type: none"> SR.2.8 SR.2.9 SR.2.10

CG NIS : « *Reference document on security measures for Operators of Essential Services* » - [link](#)

Standard/Norm

Catalogue of Measures
+ Audit & Labeling

Medium/High-end IT proficiency

Framework

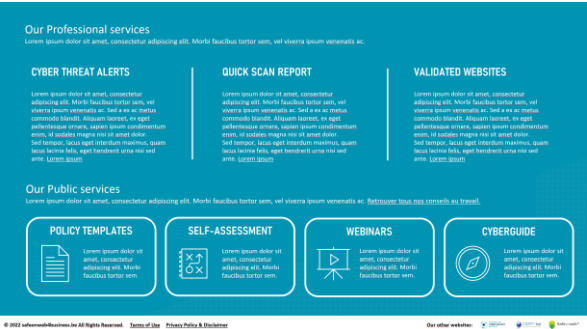
Comprehensive structure
+ Guidance on measures

Medium IT proficiency

Golden rules

Awareness on High-
priority measures

General Public



NIS 2 scope – Supervision & incident reporting

For further discussion

Options for supervision

- Audit vs. Self-assessment + Review of entity's Information Security Plans
- Centralized vs. Sectorial (or hybrid)

Options for incident reporting

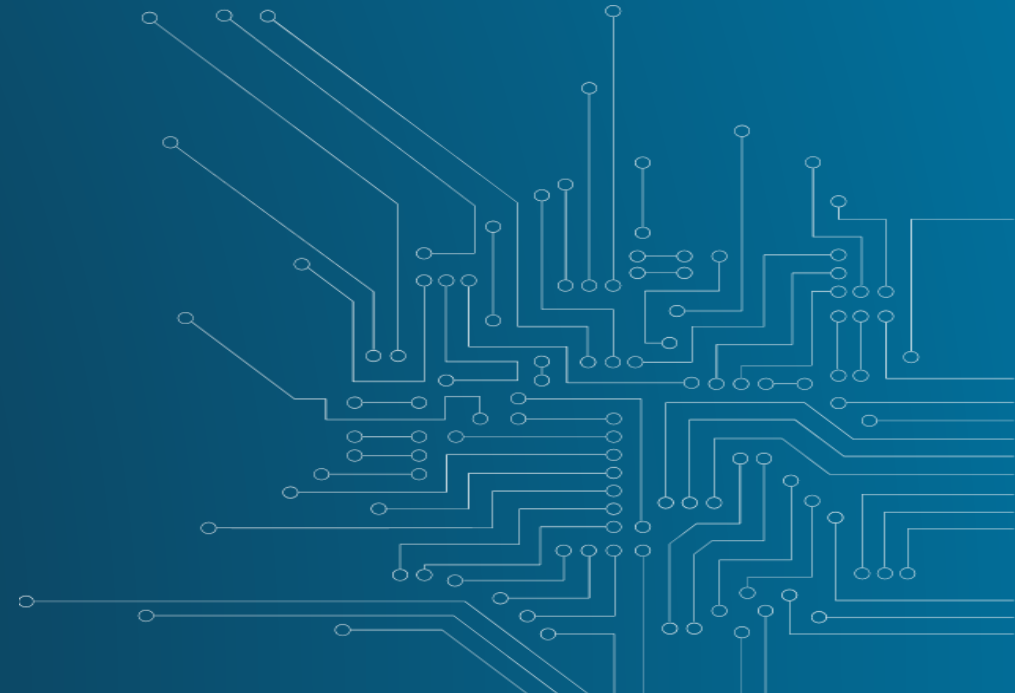
- NIS1 platform
- Incident form via portal/mail



CENTRE FOR
CYBER SECURITY
BELGIUM

Feedback or any questions?

Karl Dobbelaere (karl.dobbelaere@ccb.belgium.be)
Policy Manager, Centre for Cyber security Belgium (CCB)





CENTRE FOR
CYBER SECURITY
BELGIUM

Manageable & effective NIS security measures

May, 11, 2022

NISDUC Workshop

Karl Dobbelaere (karl.dobbelaere@ccb.belgium.be)
Policy Manager, Centre for Cyber security Belgium (CCB)

