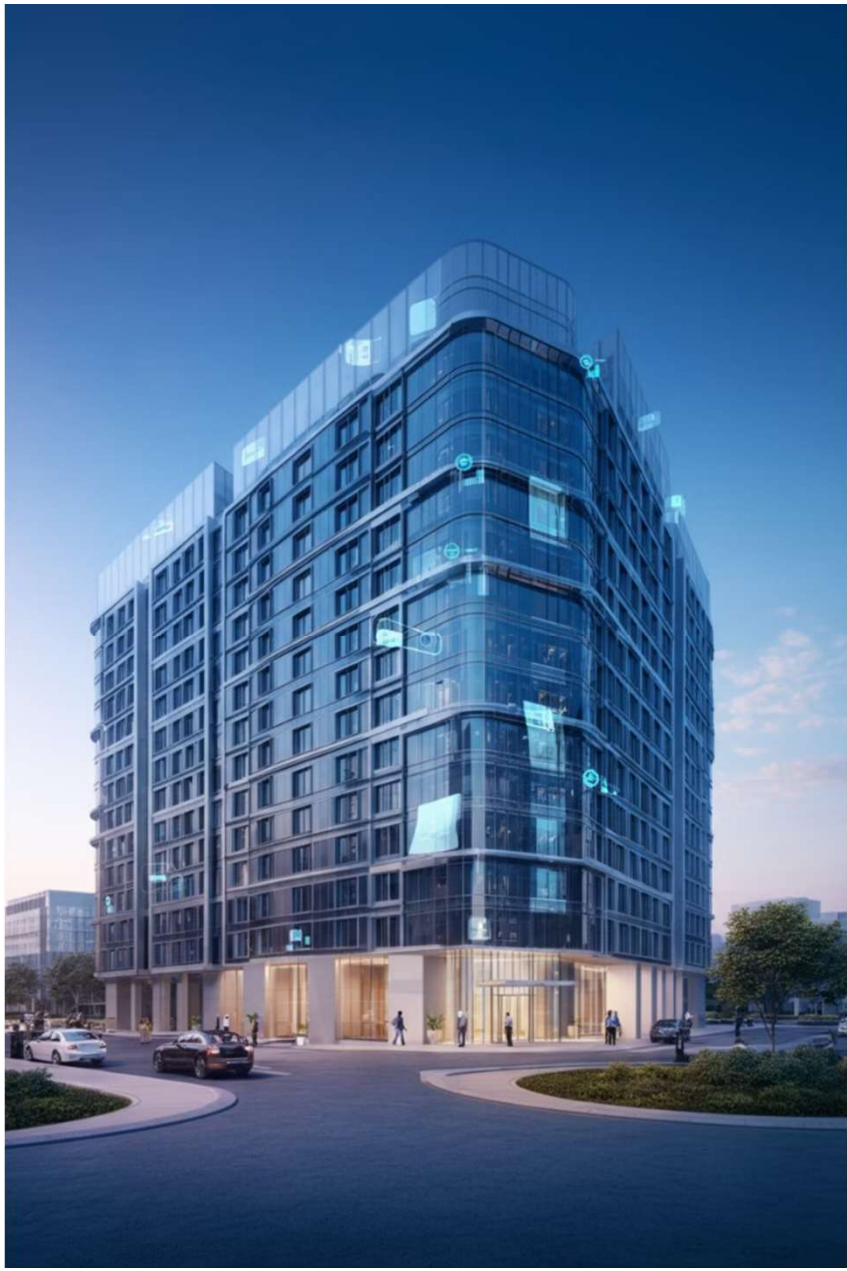
NIS2: de nieuwe interface tussen digitale en fysieke security

Bart Asnot
National Security Officer Belgium
North Europe Security Leader
Microsoft



Hackerscollectief Play verantwoordelijk voor cyberaanval op stad Antwerpen, groep dreigt om privégegevens publiek te maken

Hackerscollectief Play zit achter de cyberaanval op de stad Antwerpen. Dat zegt de groep zelf op haar website op het darkweb en onderzoek van VRT NWS bevestigt dat. "Play zou bij de aanval meer dan 500 gigabyte aan data veroverd hebben en dreigt ermee die op 19 december publiek te maken, als de stad Antwerpen geen losgeld betaalt", zegt VRT NWS-journalist Tim Verheyden.

“If you throw a frog in a pot of boiling water, it will hop right out.
But if you put that frog in a pot of tepid water and slowly warm it, the frog doesn't figure out what going on until it's too late: boiled frog.
It's just a matter of working by slow degrees.”

Verschillende websites van steden en provincies offline door cyberaanval van pro-Russische groep

Verschillende websites van Belgische provincies en steden hebben deze voormiddag een tijdlang plat gelegen door een cyberaanval. Het gaat om een zogenoemde DDoS-aanval. Onder andere de sites van de provincies Limburg en Oost-Vlaanderen en die van de steden Brussel en Luik werden geviseerd. Ondertussen zijn de meeste sites terug bereikbaar, laat het Centrum voor Cybersecurity weten.

"Overheid werd bestookt vanuit 29 landen": dit weten we nu over de "nooit geziene" cyberaanval in ons land

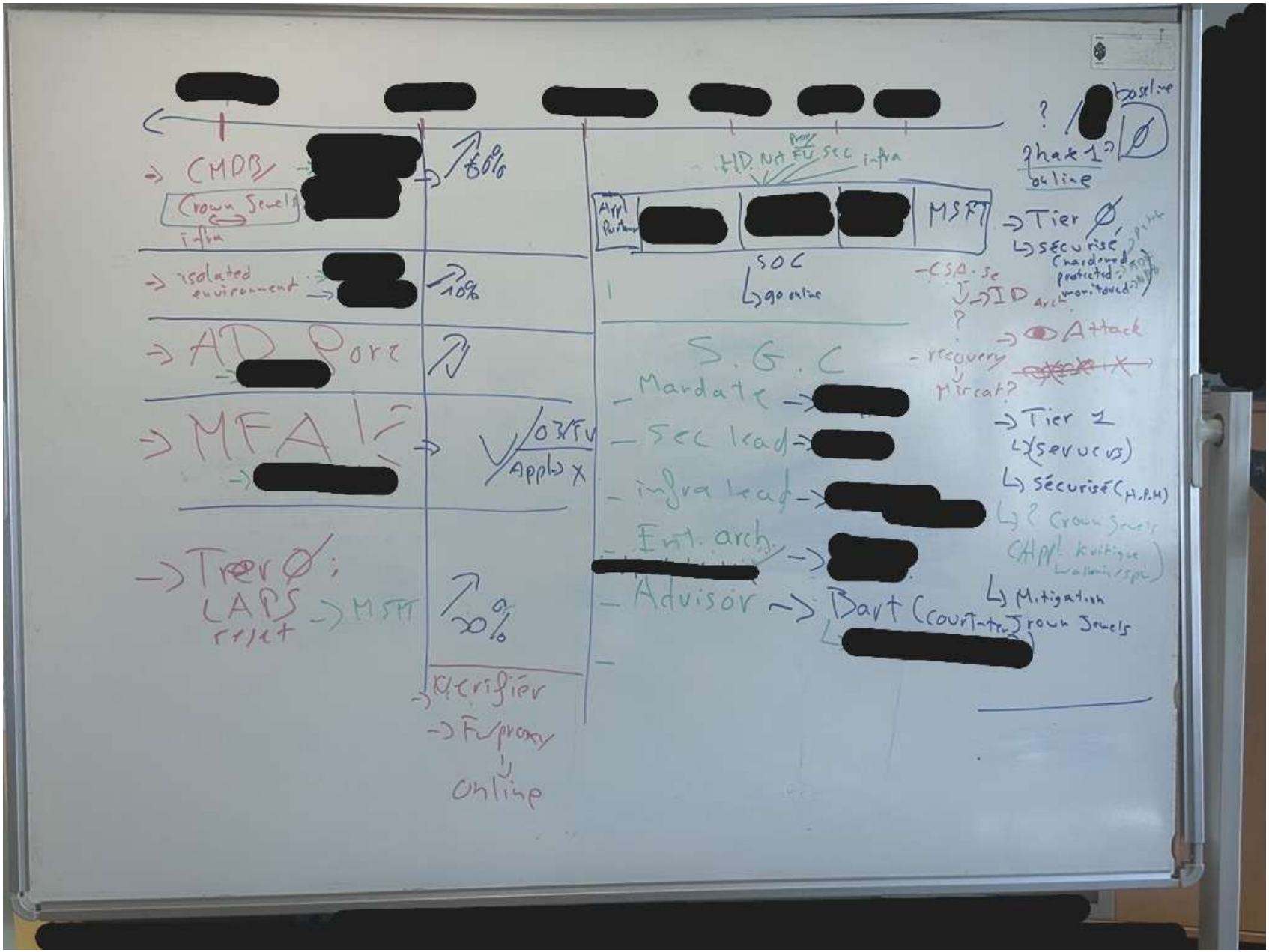
Een ongeziene cyberaanval heeft gisteren grote internetproblemen veroorzaakt, waardoor websites van overheidsinstellingen en universiteiten hinder ondervonden. Volgens de getroffen provider Belnet ging het om een cyberaanval "van nooit geziene grootte". Wat was er precies aan de hand? Wat zijn de gevolgen? En wie zit achter de aanval?

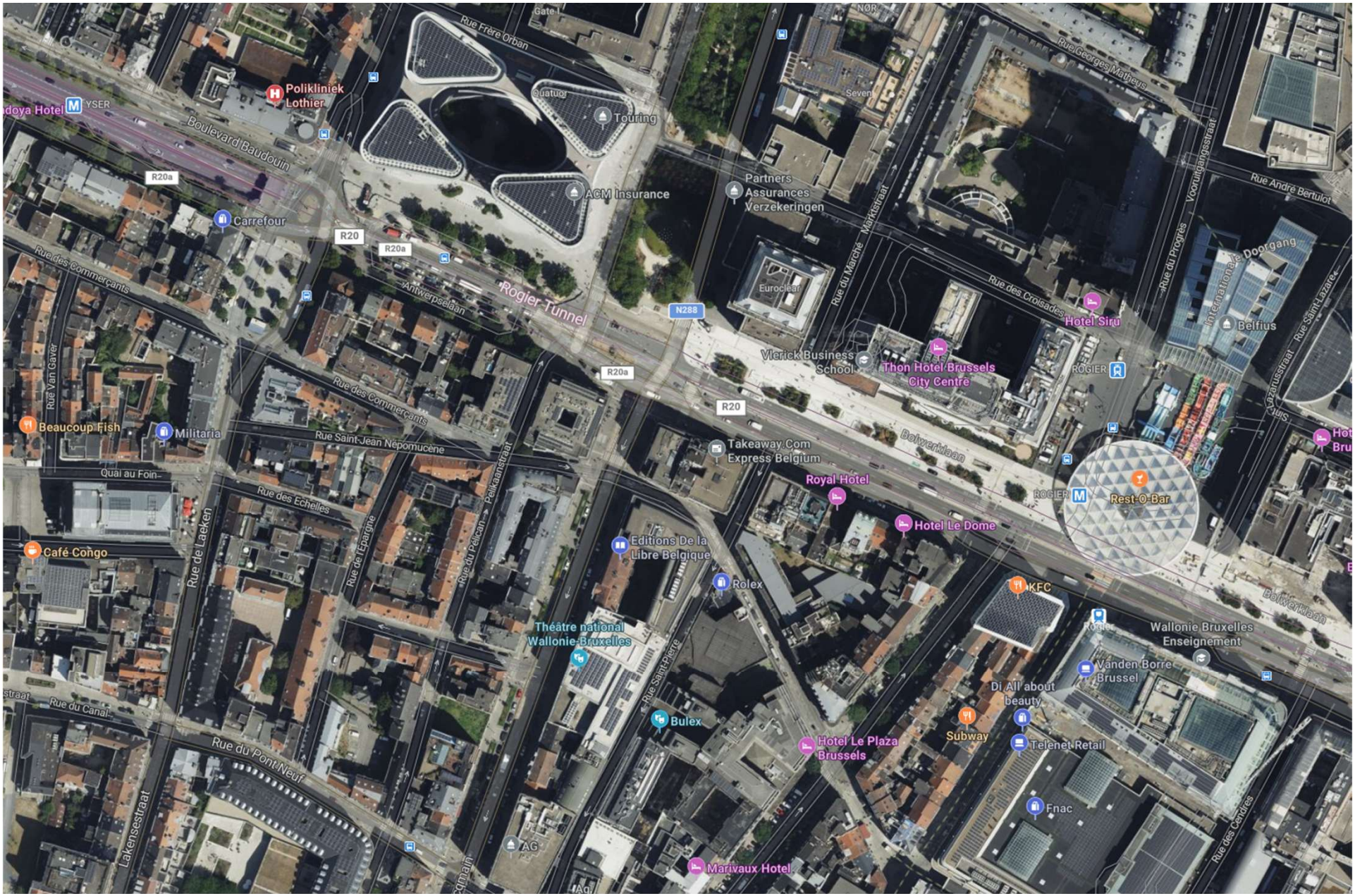
Defensie slachtoffer van zware cyberaanval, deel netwerk al dagen plat

Het leger kampt al sinds vorige donderdag met de gevolgen van een zware cyberaanval. Een deel van het computernetwerk kan voorlopig niet gebruikt worden, zegt de woordvoerder. Zo ligt het mailsysteem al enkele dagen plat. De computeraanval kwam er na een veiligheidslek in de software dat pas vorige week ontdekt werd. Het is niet duidelijk wie achter de computeraanval op Defensie zit.

Servers van kanselarij van premier De Croo mogelijk gehackt, maar "geen gegevens gestolen"

Het federaal parket is een onderzoek gestart naar een poging tot hacking van de servers van de kanselarij. Dat zijn de diensten van premier Alexander De Croo (Open VLD) waar heel wat gevoelige informatie wordt opgeslagen. Het nieuws werd gemeld door Het Nieuwsblad en wordt bevestigd door het federaal parket aan VRT NWS. "Er zijn geen gegevens gestolen", stelt Miguel de Bruycker van het Centrum voor Cybersecurity gerust.


CMDB
Crown Jewels
isolated environment
AD Port
MFA
Tier 0
LAPS
reject
MSFT
80%
10%
20%
Verifier
FU proxy
online
HD
NA
FU
Proxy
Sec
infra
App
Partner
MSFT
SOC
go online
S.G.C
Mandate
Sec lead
infra lead
Ent. arch.
Advisor
Bart (court-tru
Crown Jewels
baseline
online
Tier
Sécurisé
Attack
recovery
Tier 1
Sécurisé
Crown Jewels
Mitigation


Rue Frère Orban
Gate 1
Polikliniek Lothier
Quatuor
Touring
Seven
Rue Georges Matheys
YSER
Boulevard Baudouin
R20a
ACM Insurance
Partners Assurances Verzekeringen
Marktstraat
Voorurgangsstraat
Rue André Bertulot
Carrefour
R20
Rue du Marché
Rue du Progrès
Rue des Commerçants
Antwerpselaan
Rogier Tunnel
N288
Euroclear
Rue des Croisades
Hotel Siru
Internationale Doorgang
Belfius
Vlerick Business School
Thon Hotel Brussels City Centre
ROGIER
Lazarusstraat
Rue Saint-Lazare
Rue Van Gaver
Beaucoup Fish
Militaria
Rue Saint-Jean Népomucène
Takeaway Com Express Belgium
Boulevard Bolwerklaan
Quai au Foin
Royal Hotel
Rest-O-Bar
Rue des Echelles
Hotel Le Dome
Rue de l'Epargne
Rue du Pélican
Pelikaanstraat
Editions De la Libre Belgique
Café Congo
Rue de Laeken
Rolex
KFC
Théâtre national Wallonie-Bruxelles
Wallonie Bruxelles Enseignement
Vanden Borre Brussel
Rue Saint-Pierre
Di All about beauty
Rue du Canal
Bulex
Subway
Hotel Le Plaza Brussels
Telenet Retail
Rue du Pont Neuf
Fnac
Lakensestraat
AG
Marivaux Hotel
Rue des Cendres

What does NIS 2 mean for you?

Cybersecurity Risk Management Measures

1. **Risk management**
2. **Policies on** risk analysis and information system security
3. **Incident handling** (prevention, detection & response to incidents)
4. **Business continuity** (DR, BM, crisis management)
5. **Supply chain security** (consider supplier vulnerabilities)
6. **Vulnerability handling and management**
7. policies and procedures to assess the effectiveness of **cybersecurity risk-management measures**;
8. The use of **cryptography and encryption** where warranted
9. Basic **cybersecurity hygiene practices** & **training**
10. The use of **MFA** or continuous authentication, **secured voice/video/text communications**, **emergency comms**

Incident Reporting Obligations

Report incidents with significant* impact on the provision of services

- Within **24 hours**
- Within **72 hours** an extensive report
- Within **1 month** a final report/progress report

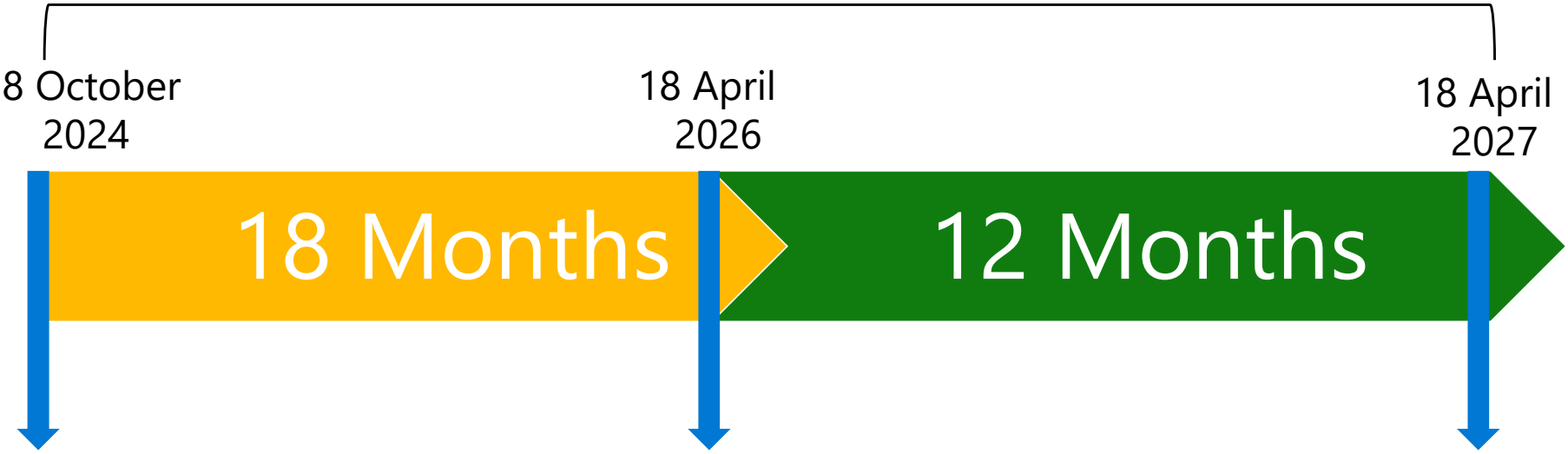
*= A significant incident is defined as: "any incident has a significant impact on the provision of services in the sectors or subsectors listed in the annexes of the NIS2 law, and which:

1. has caused or is likely to cause serious disruption to the operation of any of the services in the sectors or subsectors listed in Annexes I and II or financial loss to the concerned entity; or
2. has caused, or is likely to cause, significant material, personal or non-material damage to other natural or legal persons".

From Europe to Belgium

Timeline NIS2 implementation Belgium

30 months



Coming into Force NIS2 Legislation or identification

Ass. Level Basic or Important

- Deadline for Verification by CAB **or** ISO 27k1 Scope & SoA

Alternative

CCB/NCCA inspection

- CyFun Self-Assessment **or**
- Inform. Beveiligingsbeleid (P.S.I) + ISO 27k1 scope & SoA

Ass. Level Essential

- Deadline for Certification by CAB **or** ISO 27k1 Scope & SoA

Alternative

CCB/NCCA inspection State of Affairs:

- CyFun Self-Assessment **or**
- Inform. Beveiligingsbeleid (P.S.I) + ISO 27k1 scope & SoA

Reference: CCB presentation on BCSC Workgroup

NIS 2 Regime Belgium

	Essential Entities	Important Entities
Security Requirements	Risk based security obligations and measures: all hazard approach referenced in legal text	
Reporting Obligations	Significant incidents	
Supervision	Ex-Ante and ex-Post	Ex-Post
Sanctions	Minimum list of administrative sanctions including fines. For essential entities: possibility to suspend authorization or impose temporary ban on managerial duties	
Jurisdiction	By default: MS where the entities are established. Exception: MS where the provide services; SOC services running in country; certain digital infra and digital providers – main sub established in the EU	

ISO 27001:2022 Framework

Scope and Coverage:

International framework for establishing, implementing, maintaining, and continually improving an information security management system applicable to any organization, regardless of size, type, or industry.

Framework Structure:

Structured approach with clauses outlining requirements for establishing, implementing, maintaining, and improving an ISMS.

Compliance Requirements:

Specifies requirements for organizations to achieve certification, focusing on risk management, security controls, and continuous improvement.

Integration with NIS2 requirements:

ISO 27001 has been one acceptable path to demonstrate compliance with NIS requirements in Belgium since version one which was in place since May 2019 and remains for NIS2.

Adoption and Implementation:

Widely adopted by organizations, it offers flexibility in implementation to suit diverse organizational contexts and requirements.

Cyber Fundamentals (CyFun) Framework

Scope and Coverage:

Based on NIST Cybersecurity framework (version1), it was customized by CCB to address cybersecurity needs of organizations providing critical and important services in Belgium.

Framework Structure:

Categories or domains of cybersecurity controls, covering areas such as access control, network security, incident response, and data protection.

Compliance Requirements:

Specific cybersecurity measures and practices, including additional requirements or guidance beyond what is covered by ISO 27001.

Integration with NIS2 requirements:

Offers explicit guidance and requirements to align with NIS2 Directive.

Adoption and Implementation:

May vary across different sectors and organizations with diverse cybersecurity maturity levels and compliance outcomes compared to ISO 27001.

Effectiveness and Resilience:

Both ISO 27001:2022 and CyFun aim to enhance cybersecurity effectiveness and resilience, but the specific measures and approaches prescribed by each framework may differ based on their respective requirements, priorities, and focus areas, potentially influencing the overall cybersecurity posture and response capabilities of organizations adopting them.

CENTRE FOR CYBERSECURITY BELGIUM

Scope Assessment

The following questions aim to determine if your organisation may potentially be in scope of the Belgian NIS2 legislation. Depending on its size and the service provided, your organisation may be considered as an **essential** or **important** entity.

More information about the NIS2 law can be found here

A. Organisation size ("size-cap")

(i) Further information

Please select the size of your organisation before continuing.

These thresholds are calculated on the basis of the figures for the entire legal entity (including all its activities, even outside of the EU), proportionately consolidated with the figures from its partner or linked enterprises.
For more details on the method for calculating these thresholds, see the annex I of Commission Recommendation 2003/361/CE of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, the guide released by the European Commission, or its online tool (linked below).

Link to Commission Recommandation 2003/361/EC
Link to the "User guide on the SME definition" from the European Commission
Link to the SME self-assessment tool from the European Commission

Select your staff headcount range (in full-time equivalents - FTE):	>= 250 FTE
Select your turnover range:	> 50 million € annual turnover
Select your balance sheet total:	> 43 million € annual balance sheet total
Your organisation's size :	Large Enterprise

CyFun-Toolbox

To facilitate the use of the CyberFundamentals Framework, **several tools are provided to assist in the implementation of the framework**:

- CyFun Selection Tool is a tool for risk assessment resulting in a well-informed selection of the appropriate CyberFundamentals Assurance Level.
- CyFun Self-Assessment tool is a MS Excel format tool to prepare self-assessment and includes spider diagrams to support management reporting
- CyberFundamentals Framework mapping provides an overview of the requirements and links with the frameworks in a MS Excel-format

Small

The starting level **Small** allows an organisation to make an initial assessment. It is intended for micro-organisations or organisations with limited technical knowledge.

pdf

Download

40 lines in CyFun SA toolbox

Basic

The assurance level **Basic** contains the standard information security measures for all enterprises. These provide an effective security value with technology and processes that are generally already available. Where justified, the measures are tailored and refined.

pdf

Download

146 lines in CyFun SA toolbox

Important

The assurance level **Important** is designed to minimise the risks of targeted cyber-attacks by actors with common skills and resources in addition to known cyber security risks.

pdf

Download

228 lines in CyFun SA toolbox

Essential

The assurance level **Essential** goes one step further and is designed to address the risk of advanced cyber-attacks by actors with extensive skills and resources.

pdf

Download

	CyberFundamentals Categories	Target Maturity Score	Category Maturity Score	Documentation Maturity Score	Implementation Maturity Score
	Overall	3.50		1.00	1.01
IDENTIFY	Asset Management (ID.AM)	3.00	1.12	1.07	1.17
	Business Environment (ID.BE)	3.00	1.00	1.00	1.00
	Governance (ID.GV)	3.00	1.00	1.00	1.00
	Risk Assessment (ID.RA)	3.00	1.00	1.00	1.00
	Risk Management Strategy (ID.RM)	3.00	1.00	1.00	1.00
	Supply Chain Risk Management (ID.SC)	3.00	1.00	1.00	1.00
PROTECT	Identity Management, Authentication and Access Control (PR.AC)	3.00	1.00	1.00	1.00
	Awareness and Training (PR.AT)	3.00	1.00	1.00	1.00
	Data Security (PR.DS)	3.00	1.00	1.00	1.00
	Information Protection Processes and Procedures (PR.IP)	3.00	1.00	1.00	1.00
	Maintenance (PR.MA)	3.00	1.00	1.00	1.00
	Protective Technology (PR.PT)	3.00	1.00	1.00	1.00
DETECT	Anomalies and Events (DE.AE)	3.00	1.00	1.00	1.00
	Security Continuous Monitoring (DE.CM)	3.00	1.00	1.00	1.00
	Detection Processes (DE.DP)	3.00	1.00	1.00	1.00
RESPOND	Response Planning (RS.RP)	3.00	1.00	1.00	1.00
	Communications (RS.CO)	3.00	1.00	1.00	1.00
	Analysis (RS.AN)	3.00	1.00	1.00	1.00
	Mitigation (RS.MI)	3.00	1.00	1.00	1.00
	Improvements (RS.IM)	3.00	1.00	1.00	1.00
RECOVER	Recovery Planning (RC.RP)	3.00	1.00	1.00	1.00
	Improvements (RC.IM)	3.00	1.00	1.00	1.00
	Communications (RC.CO)	3.00	1.00	1.00	1.00

	CyberFundamentals Categories	Target Maturity Score	Category Maturity Score	Documentation Maturity Score	Implementation Maturity Score
	Overall	3.50		1.00	1.01
IDENTIFY	Asset Management (ID.AM)	3.00	1.12	1.07	1.17
	Business Environment (ID.BE)	3.00	1.00	1.00	1.00
	Governance (ID.GV)	3.00	1.00	1.00	1.00
	Risk Assessment (ID.RA)	3.00	1.00	1.00	1.00
	Risk Management Strategy (ID.RM)	3.00	1.00	1.00	1.00
	Supply Chain Risk Management (ID.SC)	3.00	1.00	1.00	1.00
PROTECT	Identity Management, Authentication and Access Control (PR.AC)	3.00	1.00	1.00	1.00
	Awareness and Training (PR.AT)	3.00	1.00	1.00	1.00
	Data Security (PR.DS)	3.00	1.00	1.00	1.00
	Information Protection Processes and Procedures (PR.IP)	3.00	1.00	1.00	1.00
	Maintenance (PR.MA)	3.00	1.00	1.00	1.00
	Protective Technology (PR.PT)	3.00	1.00	1.00	1.00
DETECT	Anomalies and Events (DE.AE)	3.00	1.00	1.00	1.00
	Security Continuous Monitoring (DE.CM)	3.00	1.00	1.00	1.00
	Detection Processes (DE.DP)	3.00	1.00	1.00	1.00
RESPOND	Response Planning (RS.RP)	3.00	1.00	1.00	1.00
	Communications (RS.CO)	3.00	1.00	1.00	1.00
	Analysis (RS.AN)	3.00	1.00	1.00	1.00
	Mitigation (RS.MI)	3.00	1.00	1.00	1.00
	Improvements (RS.IM)	3.00	1.00	1.00	1.00
RECOVER	Recovery Planning (RC.RP)	3.00	1.00	1.00	1.00
	Improvements (RC.IM)	3.00	1.00	1.00	1.00
	Communications (RC.CO)	3.00	1.00	1.00	1.00

Reconnaissance

Command & Control

Infiltration

Left Of Bang

Actions on Objectives

Function	Category	Key Measure	Physical Security	Subcategory	Requirement	Guidance
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.		y	**ID.AM-3:** Organizational communication and data flows are mapped	**BASIC_ID.AM-3.1**: Information that the organization stores and uses shall be identified.	any useful way that makes sense to your business. You may want to have your employees make a list of all the information they use in their regular activities. List everything you can think of, but you do not need to be too specific. For example, you may keep customer names and email addresses, receipts for raw material, your banking information, or other proprietary information. •Consider mapping this information with the associated assets identified in the inventories of physical devices, systems, software platforms and applications used within the organization (see ID.AM-1 & ID.AM-2).
			y		**IMPORTANT_ID.AM-3.2**: All connections within the organization's ICT/OT environment, and to other organization-internal platforms shall be mapped, documented, approved, and updated as appropriate.	•Connection information includes, for example, the interface characteristics, data characteristics, ports, protocols, addresses, description of the data, security requirements, and the nature of the connection. •Configuration management can be used as supporting asset. •This documentation should not be stored only on the network it represents. •Consider keeping a copy of this documentation in a safe offline environment (e.g. offline hard disk, paper hardcopy, …)
			y		**ID.AM-3.3**: The information flows/data flows within the organization's ICT/OT environment, as well as to other organization-internal systems shall be mapped, documented, authorized, and updated when changes occur.	•With knowledge of the information/data flows within a system and between systems, it is possible to determine where information can and cannot go. •Consider: oEnforcing controls restricting connections to only authorized interfaces. oHeightening system monitoring activity whenever there is an indication of increased risk to organization's critical operations and assets. oProtecting the system from information leakage due to electromagnetic signals emanations.
			y	**ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**BASIC_ID.AM-5.1**: The organization's resources (hardware, devices, data, time, personnel, information, and software) shall be prioritized based on their classification, criticality, and business value.	•Determine organization's resources (e.g., hardware, devices, data, time, personnel, information, and software): oWhat would happen to my business if these resources were made public, damaged, lost…? oWhat would happen to my business when the integrity of resources is no longer guaranteed? oWhat would happen to my business if I/my customers couldn't access these resources? And rank these resources based on their classification, criticality, and business value. •Resources should include enterprise assets.
			y			•Create a classification for sensitive information by first determining categories, e.g. oPublic - freely accessible to all, even externally oInternal - accessible only to members of your organization oConfidential - accessible only to those whose duties require access. •Communicate these categories and identify what types of data fall into these categories (HR data, financial data, legal data, personal data, etc.). •Consider the use of the Traffic Light Protocol (TLP). •Data classification should apply to the three aspects: C-I-A.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities,		y	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	**ID.BE-1.2**: The organization shall protect its ICT/OT environment from supply chain threats by applying security safeguards as part of a documented comprehensive security strategy	No additional guidance on this topic.
			y	**ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g. under	**ID.BE-5.2**: Information processing & supporting facilities shall implement redundancy to meet availability requirements, as defined by the	•Consider provisioning adequate data and network redundancy (e.g. redundant network devices, servers with load balancing, raid arrays, backup services, 2 separate datacentres, fail-over network connections, 2 ISP's…). •Consider protecting critical equipment/services from power outages and other failures due to utility

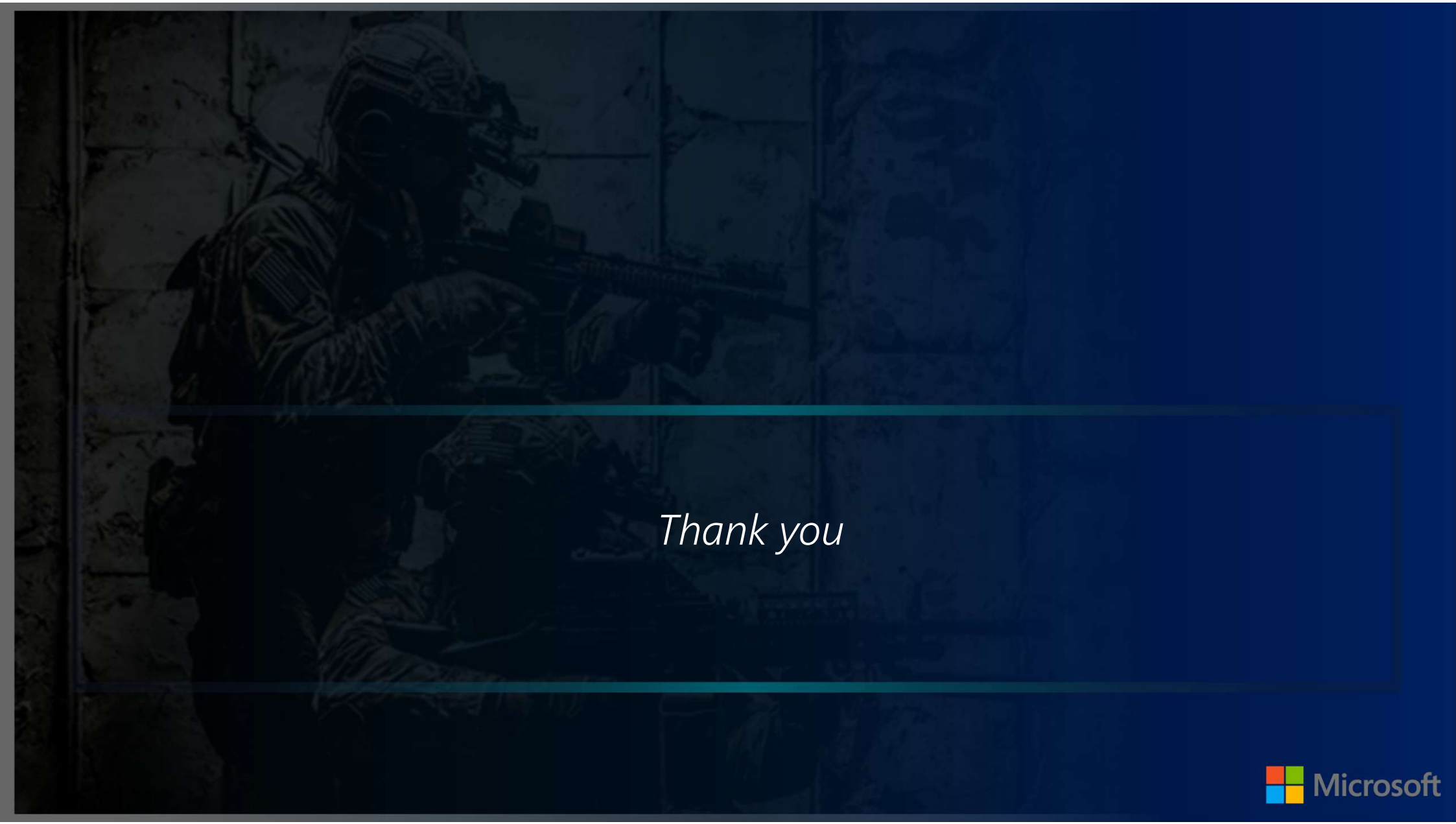
Function	Category	Key Measure	Physical Security	Subcategory	Requirement	Guidance
DETECT (DE)	**Security Continuous Monitoring (DE.CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.		y	cybersecurity events	critical systems and devices shall be, on top of the physical access monitoring to the facility, increased through physical intrusion alarms, surveillance equipment, independent surveillance teams.	It is recommended to log all visitors.
			y	**DE.CM-6**: External service provider activity is monitored to detect potential cybersecurity events	**IMPORTANT_DE.CM-6.2**: External service providers' conformance with personnel security policies and procedures and contract security requirements shall be monitored relative to their cybersecurity risks.	No additional guidance on this topic.
			y	**DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed	**IMPORTANT_DE.CM-7.1**: The organization's business critical systems shall be monitored for unauthorized personnel access, connections, devices, access points, and software.	•Unauthorized personnel access includes access by external service providers. •System inventory discrepancies should be included in the monitoring. •Unauthorized configuration changes to organization's critical systems should be included in the monitoring.
			y		**DE.CM-7.2**: Unauthorized configuration changes to organization's systems shall be monitored and addressed with the appropriate mitigation actions.	No additional guidance on this topic.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.		y	**DE.DP-5:** Detection processes are continuously improved	**DE.DP-5.2**: The organization shall conduct specialized assessments including in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing on the organization's critical systems.	These activities can be outsourced, preferably to accredited organizations.
RESPOND	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.		y	**RS.RP-1:** Response plan is executed during or after an incident	**BASIC_RS.RP-1.1**: An incident response process, including roles, responsibilities, and authorities, shall be executed during or after an information/cybersecurity event on the organization's critical systems.	•The incident response process should include a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack. •The roles, responsibilities, and authorities in the incident response plan should be specific on involved people, contact info, different roles and responsibilities, and who makes the decision to initiate recovery procedures as well as who will be the contact with appropriate external stakeholders.
			y			It should be considered to determine the causes of an information/cybersecurity event and implement a corrective action in order that the event does not recur or occur elsewhere (an infection by malicious code on one machine did not have spread elsewhere in the network). The effectiveness of any corrective action taken should be reviewed. Corrective actions should be appropriate to the effects of the information/cybersecurity event encountered. **Internal Note:** Requirements are covered in PR.IP-9
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).		y	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**IMPORTANT_RS.CO-1.1**: The organization shall ensure that personnel understand their roles, objectives, restoration priorities, task sequences (order of operations) and assignment responsibilities for event response.	Consider the use the CCB Incident Management Guide to guide you through this exercise and consider bringing in outside experts if needed. Test your plan regularly and adjust it after each incident.
			y	**RS.CO-4:** Coordination with stakeholders occurs consistent with response plans	**IMPORTANT_RS.CO-4.1**: The organization shall coordinate information/cybersecurity incident response actions with all predefined stakeholders.	•Stakeholders for incident response include for example, mission/business owners, organization's critical system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices. •Coordination with stakeholders occurs consistent with incident response plans.

People controls (8)

Confidentiality or non-disclosure agreements	A.6.6
Disciplinary process	A.6.4
Information security awareness, education and tr...	A.6.3
Information security event reporting	A.6.8
Remote working	A.6.7
Responsibilities after termination or change of e...	A.6.5
Screening	A.6.1
Terms and conditions of employment	A.6.2

Physical controls (14)

Cabling security	A.7.12
Clear desk and clear screen	A.7.7
Equipment maintenance	A.7.13
Equipment siting and protection	A.7.8
Physical entry	A.7.2
Physical security monitoring	A.7.4
Physical security perimeters	A.7.1
Protecting against physical and environmental th...	A.7.5
Secure disposal or re-use of equipment	A.7.14
Securing offices, rooms and facilities	A.7.3
Security of assets off-premises	A.7.9
Storage media	A.7.10
Supporting utilities	A.7.11
Working in secure areas	A.7.6


Thank you
Microsoft