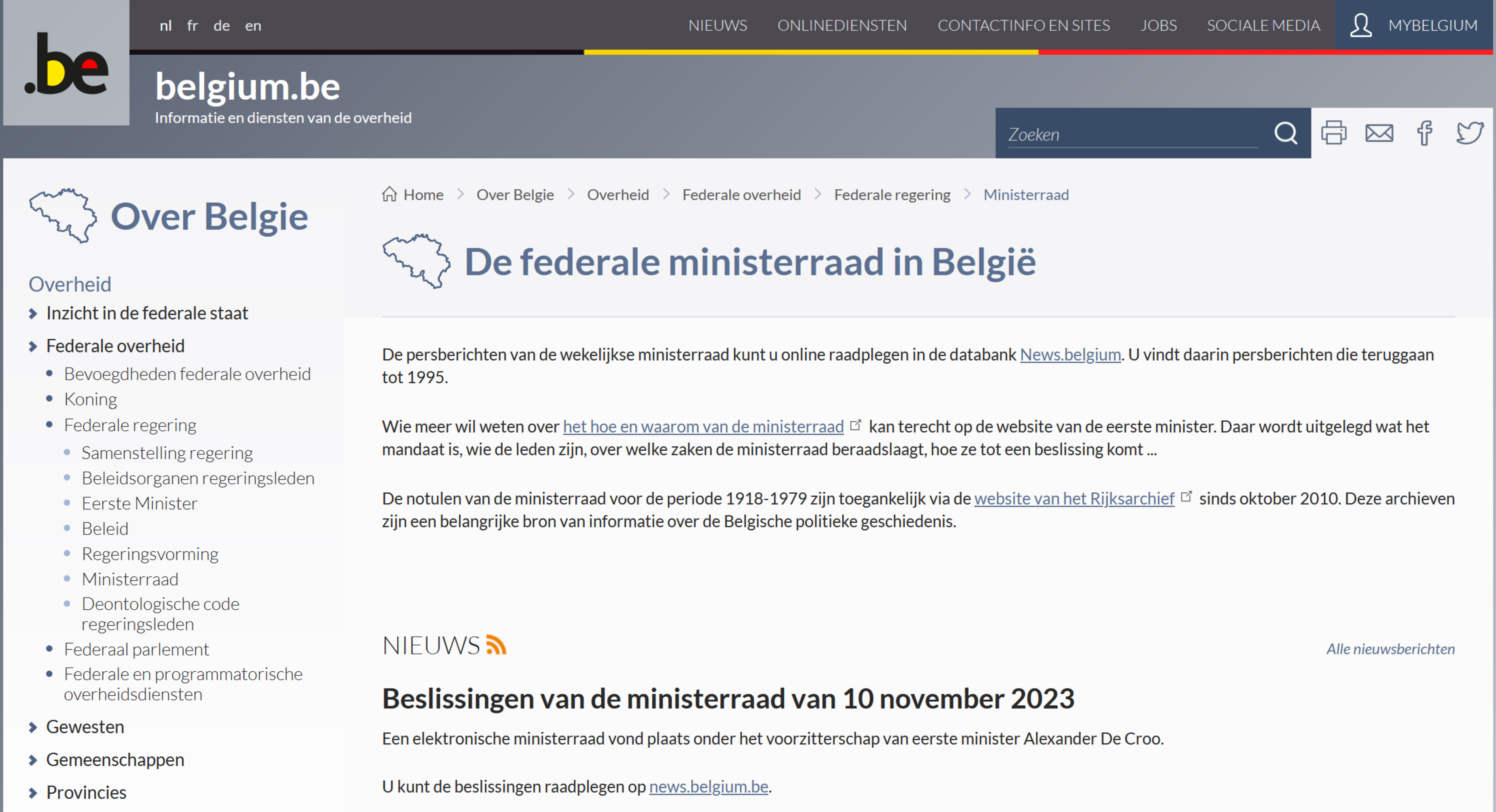
NIS2

Belangrijkste regels en hoe aanpakken



Over Belgie

Overheid

- Inzicht in de federale staat
- Federale overheid
  - Bevoegdheden federale overheid
  - Koning
  - Federale regering
    - Samenstelling regering
    - Beleidsorganen regeringsleden
    - Eerste Minister
    - Beleid
    - Regeringsvorming
    - Ministerraad
    - Deontologische code regeringsleden
  - Federaal parlement
  - Federale en programmatorische overheidsdiensten
- Gewesten
- Gemeenschappen
- Provincies

Home > Over Belgie > Overheid > Federale overheid > Federale regering > Ministerraad

De federale ministerraad in België

De persberichten van de wekelijkse ministerraad kunt u online raadplegen in de databank News.belgium. U vindt daarin persberichten die teruggaan tot 1995.

Wie meer wil weten over het hoe en waarom van de ministerraad kan terecht op de website van de eerste minister. Daar wordt uitgelegd wat het mandaat is, wie de leden zijn, over welke zaken de ministerraad beraadslaagt, hoe ze tot een beslissing komt ...

De notulen van de ministerraad voor de periode 1918-1979 zijn toegankelijk via de website van het Rijksarchief sinds oktober 2010. Deze archieven zijn een belangrijke bron van informatie over de Belgische politieke geschiedenis.

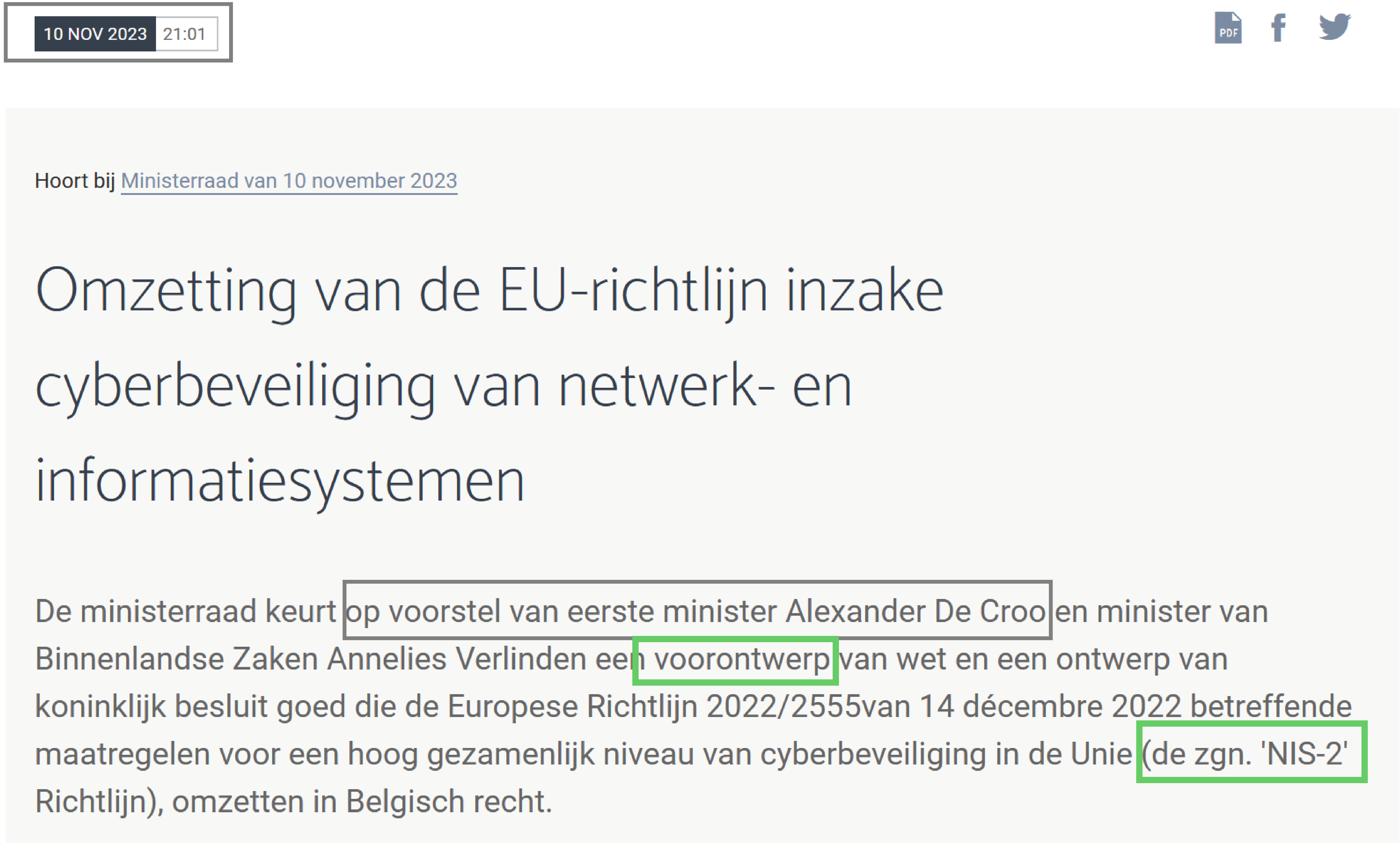
NIEUWS

Alle nieuwsberichten

Beslissingen van de ministerraad van 10 november 2023

Een elektronische ministerraad vond plaats onder het voorzitterschap van eerste minister Alexander De Croo.

U kunt de beslissingen raadplegen op news.belgium.be.



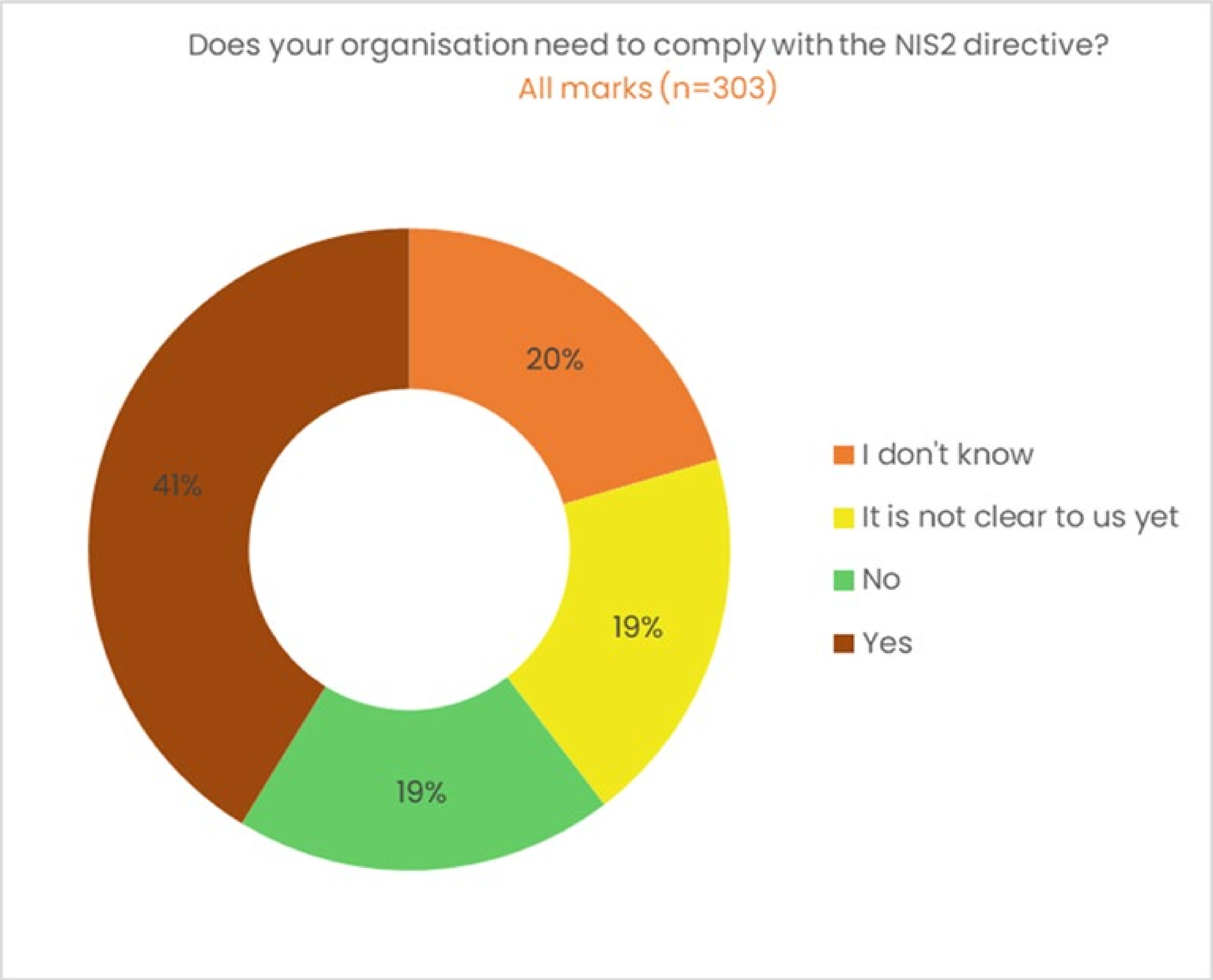
10 NOV 2023 21:01

Hoort bij Ministerraad van 10 november 2023

Omzetting van de EU-richtlijn inzake cyberbeveiliging van netwerk- en informatiesystemen

De ministerraad keurt op voorstel van eerste minister Alexander De Croo en minister van Binnenlandse Zaken Annelies Verlinden een voorontwerp van wet en een ontwerp van koninklijk besluit goed die de Europese Richtlijn 2022/2555van 14 décembre 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (de zgn. 'NIS-2' Richtlijn), omzetten in Belgisch recht.

Result of the Beltug Priorities Compass 2023



inetum realdolmen

Positive digital flow

Network and Information Security Directive **NIS2**

Overview of NIS2

European
Commission

NIS2 is the new European cybersecurity directive that will replace the existing NIS Directive as from **October 2024.**

18

180K

It is the most comprehensive EU cybersecurity legislation to date, covering 18 sectors and over 180K+ companies.

Its purpose is to establish a baseline of security measures for digital service providers and operators of essential services, to mitigate the risk of cyber attacks and to improve the overall level of cybersecurity in the EU.

Member States have until October 17, 2024 to transpose the Directive into national law.

The Network Information Security Directive
NIS2 vs. NIS1

Stronger requirements and more affected sectors

Focus on securing and business continuity. This includes supply chain security.

Improving & streamlining the report obligations.

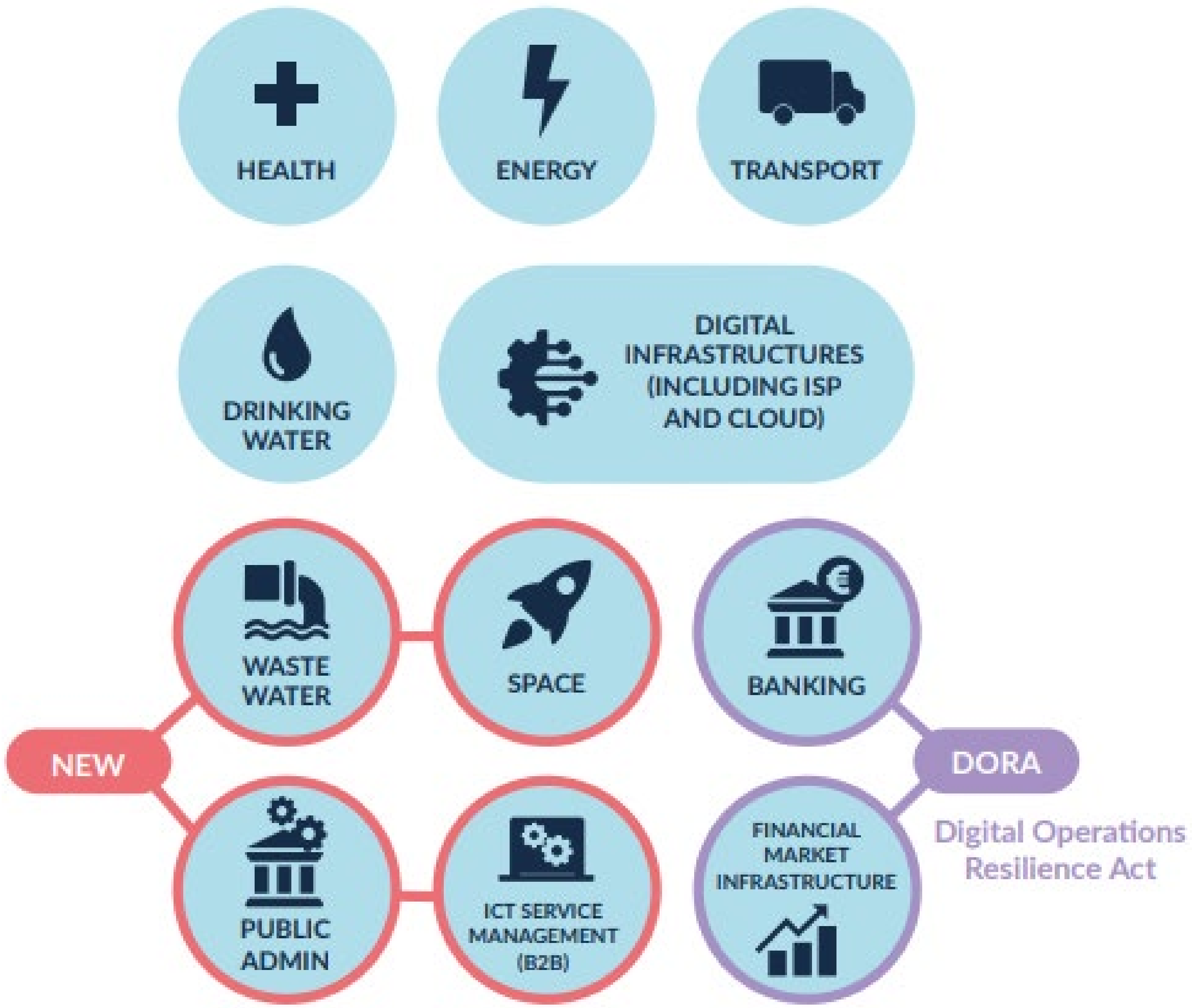
Worse Repercussions. Next to fines, NIS2 can lead to legal ramifications for management.

Enforcement localized in all European member states

NIS affects various sectors, including…

On September 14, the European Commission published new guidelines explaining which sectors will be considered critical and what they should report to national authorities in the EU under the NIS2 directive.

Highly Critical Sectors



HEALTH

ENERGY

TRANSPORT

DRINKING WATER

DIGITAL INFRASTRUCTURES (INCLUDING ISP AND CLOUD)

WASTE WATER

SPACE

BANKING

NEW

DORA

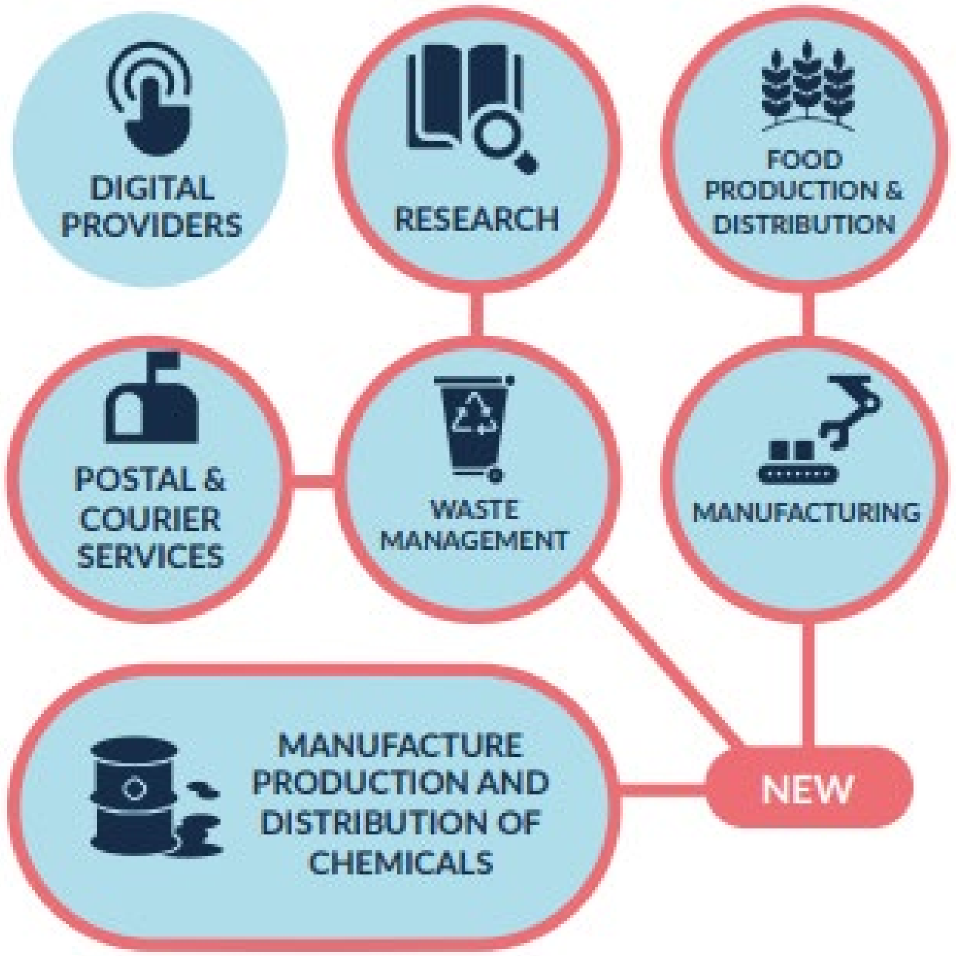
Digital Operations Resilience Act

PUBLIC ADMIN

ICT SERVICE MANAGEMENT (B2B)

FINANCIAL MARKET INFRASTRUCTURE

Critical Sectors



DIGITAL PROVIDERS

RESEARCH

FOOD PRODUCTION & DISTRIBUTION

POSTAL & COURIER SERVICES

WASTE MANAGEMENT

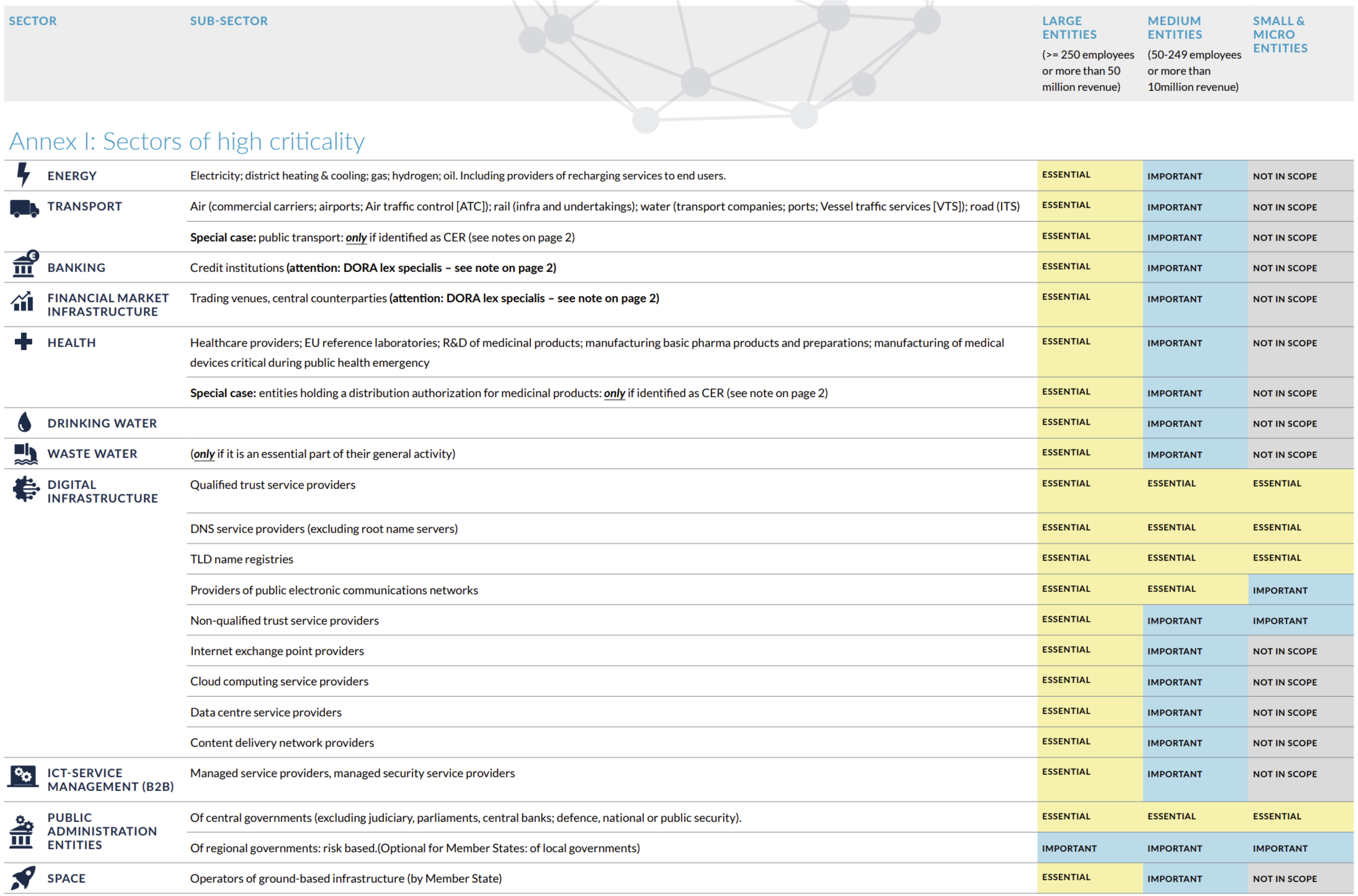
MANUFACTURING

MANUFACTURE PRODUCTION AND DISTRIBUTION OF CHEMICALS

NEW

Essential and Important entities

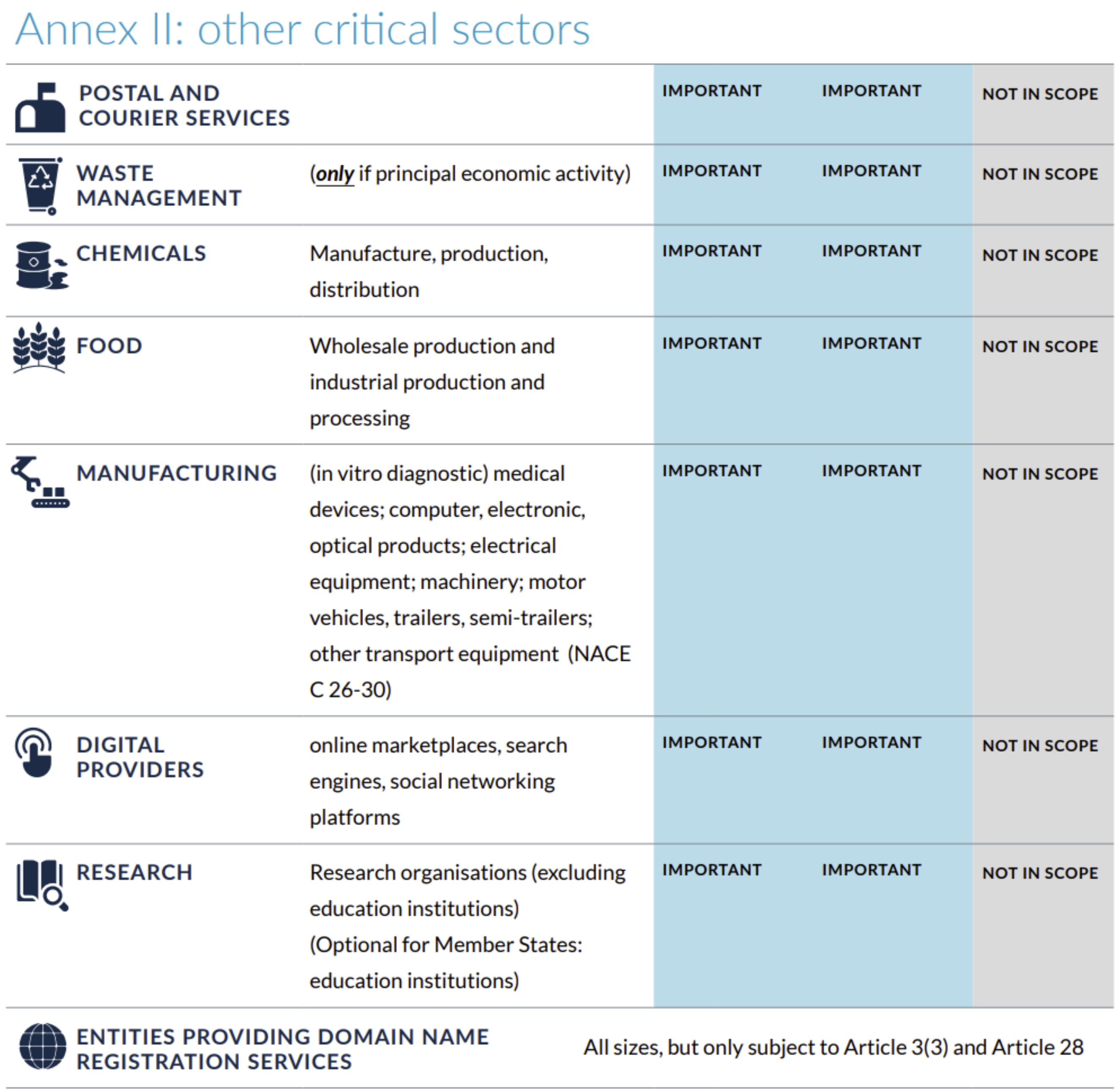
Entities may be designated as “Essential” or “Important” depending on factors such as size, sector and criticality



SECTOR	SUB-SECTOR	LARGE ENTITIES (>= 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10million revenue)	SMALL & MICRO ENTITIES
Annex I: Sectors of high criticality				
ENERGY	Electricity; district heating & cooling; gas; hydrogen; oil. Including providers of recharging services to end users.	ESSENTIAL	IMPORTANT	NOT IN SCOPE
TRANSPORT	Air (commercial carriers; airports; Air traffic control [ATC]); rail (infra and undertakings); water (transport companies; ports; Vessel traffic services [VTS]); road (ITS)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Special case: public transport: ***only*** if identified as CER (see notes on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
BANKING	Credit institutions **(attention: DORA lex specialis – see note on page 2)**	ESSENTIAL	IMPORTANT	NOT IN SCOPE
FINANCIAL MARKET INFRASTRUCTURE	Trading venues, central counterparties **(attention: DORA lex specialis – see note on page 2)**	ESSENTIAL	IMPORTANT	NOT IN SCOPE
HEALTH	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Special case: entities holding a distribution authorization for medicinal products: ***only*** if identified as CER (see note on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
DRINKING WATER		ESSENTIAL	IMPORTANT	NOT IN SCOPE
WASTE WATER	(***only*** if it is an essential part of their general activity)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
DIGITAL INFRASTRUCTURE	Qualified trust service providers	ESSENTIAL	ESSENTIAL	ESSENTIAL
	DNS service providers (excluding root name servers)	ESSENTIAL	ESSENTIAL	ESSENTIAL
	TLD name registries	ESSENTIAL	ESSENTIAL	ESSENTIAL
	Providers of public electronic communications networks	ESSENTIAL	ESSENTIAL	IMPORTANT
	Non-qualified trust service providers	ESSENTIAL	IMPORTANT	IMPORTANT
	Internet exchange point providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Cloud computing service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Data centre service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Content delivery network providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
ICT-SERVICE MANAGEMENT (B2B)	Managed service providers, managed security service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
PUBLIC ADMINISTRATION ENTITIES	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).	ESSENTIAL	ESSENTIAL	ESSENTIAL
	Of regional governments: risk based.(Optional for Member States: of local governments)	IMPORTANT	IMPORTANT	IMPORTANT
SPACE	Operators of ground-based infrastructure (by Member State)	ESSENTIAL	IMPORTANT	NOT IN SCOPE

Essential and Important entities

Entities may be designated as “Essential” or “Important” depending on factors such as size, sector and criticality



Annex II: other critical sectors

POSTAL AND COURIER SERVICES		IMPORTANT	IMPORTANT	NOT IN SCOPE
WASTE MANAGEMENT	(*only* if principal economic activity)	IMPORTANT	IMPORTANT	NOT IN SCOPE
CHEMICALS	Manufacture, production, distribution	IMPORTANT	IMPORTANT	NOT IN SCOPE
FOOD	Wholesale production and industrial production and processing	IMPORTANT	IMPORTANT	NOT IN SCOPE
MANUFACTURING	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)	IMPORTANT	IMPORTANT	NOT IN SCOPE
DIGITAL PROVIDERS	online marketplaces, search engines, social networking platforms	IMPORTANT	IMPORTANT	NOT IN SCOPE
RESEARCH	Research organisations (excluding education institutions) (Optional for Member States: education institutions)	IMPORTANT	IMPORTANT	NOT IN SCOPE
ENTITIES PROVIDING DOMAIN NAME REGISTRATION SERVICES		All sizes, but only subject to Article 3(3) and Article 28		

What does NIS2 mean for me?

Cybersecurity Risk Management Measures

Essential and Important entities must take appropriate and proportional technical, operational and organizational measures to manage the risks posed to the systems.

- Risk Analysis & Management
- Security Policies & Asset Management
- Incident handling (prevention, detection & response to incidents)
- Business continuity and crisis management
- Supply chain security consider supplier vulnerabilities
- Vulnerability handling and disclosures
- Regular assessments to determine the effectiveness of cybersecurity risk management measures (e.g., reflection of state of art – security posture)
- The use of cryptography and encryption where appropriate
- Basic cybersecurity hygiene & training
- The use of MFA or continuous authentication

Incident Reporting Obligations

Significant incidents must be notified to CSIRT without undue delay.

Report incidents with significant* impact on the provision of services

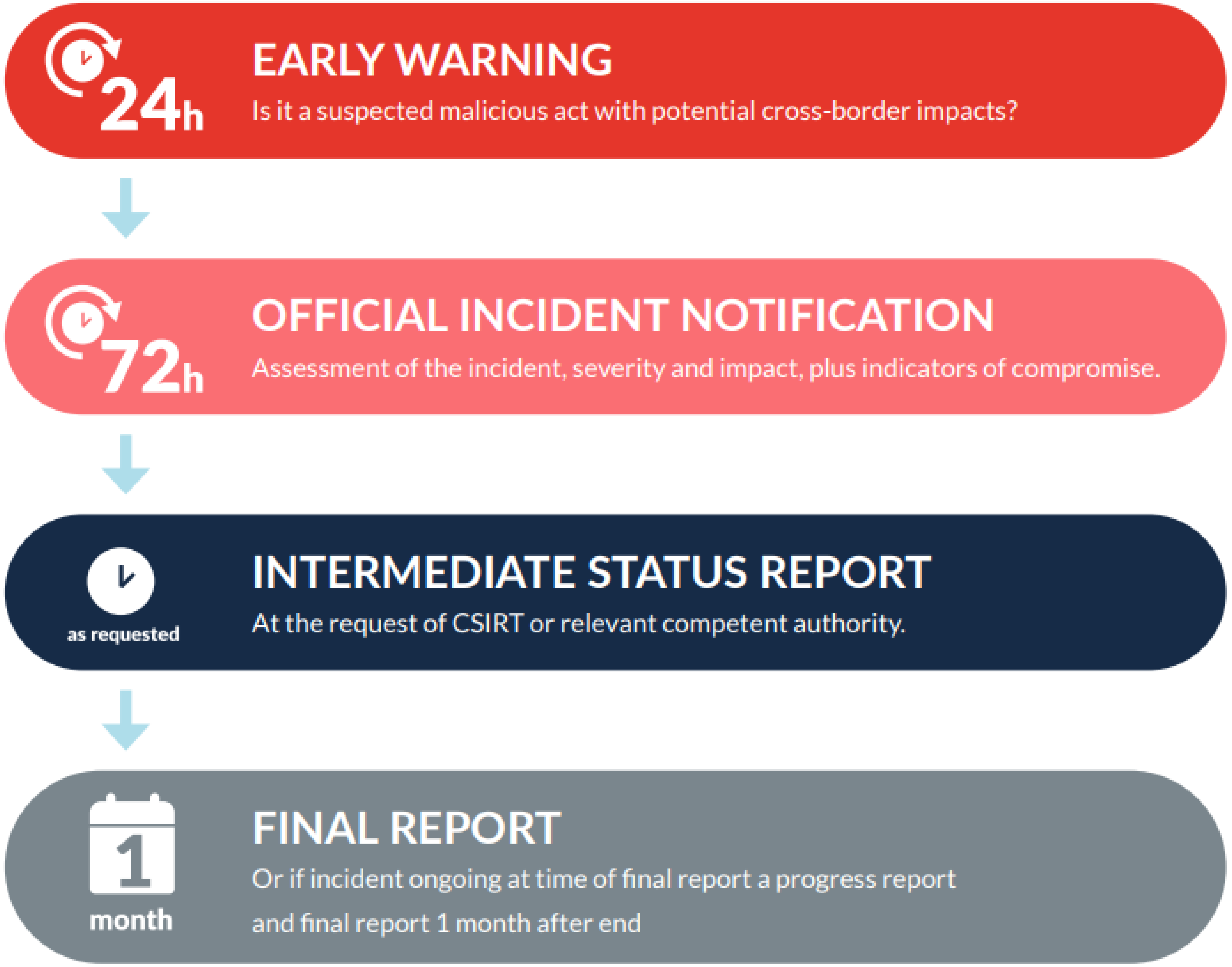
- Within 24 hours
- Within 72 hours an extensive report
- Within 1 month a final report progress report

**=An incident is significant if it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned or if it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage*

- Computer Security Incident Response Team (CSIRT)
- Competent Authority
- Recipients of services

Incident notification

NIS2 imposes notification obligations in phases, for incidents which have a ‘significant impact’ on the provision of their services. These notifications must be made to the relevant competent authority or CSIRT (Computer Security Incident Response Team).



24h

EARLY WARNING

Is it a suspected malicious act with potential cross-border impacts?

72h

OFFICIAL INCIDENT NOTIFICATION

Assessment of the incident, severity and impact, plus indicators of compromise.

as requested

INTERMEDIATE STATUS REPORT

At the request of CSIRT or relevant competent authority.

1 month

FINAL REPORT

Or if incident ongoing at time of final report a progress report and final report 1 month after end

Enforcement and Penalties

NIS2 provides national authorities with a minimum list of enforcement powers for non-compliance, including:

- Issue **warnings** for non-compliance
- Issue **binding instructions**
- Order to **cease conduct** that is non-compliant
- Order to **bring risk management measures** or reporting obligations i
- Order to **inform the natural or legal person(s)** to whom they provide s
  are potentially affected by a significant cyber threat
- Order to **implement the recommendations** provided as a result of
- Designate **a monitoring officer** with well-defined tasks to oversee
- Order to **make public** aspects of non-compliance
- Impose administrative **fines**
- An essential entities certification or authorisation concerning the service **can be suspended**
- And those responsible for discharging managerial responsibilities at chief executive officer or legal representative level can be temporarily **prohibited from exercising managerial functions**

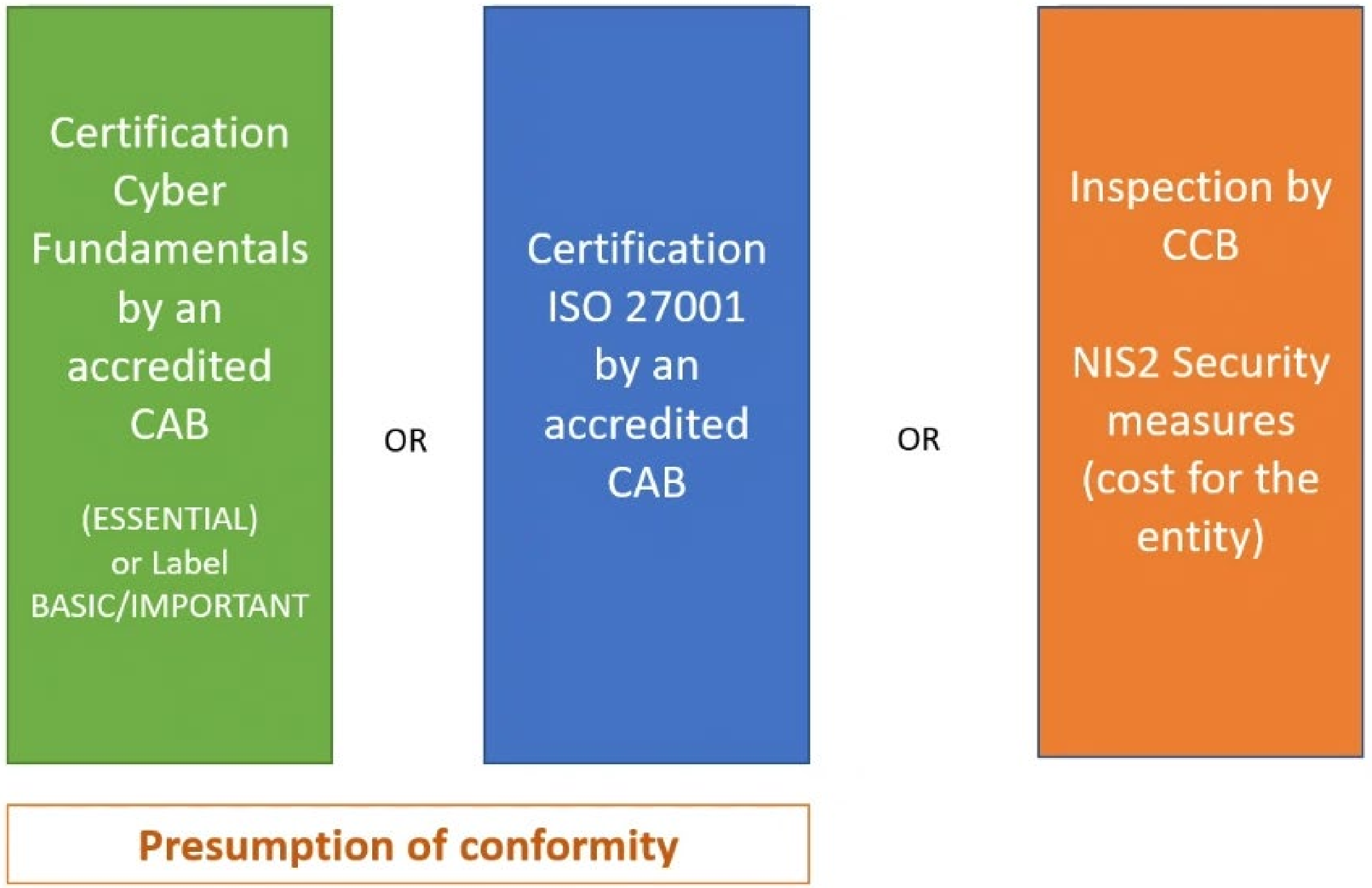
A maximum of **at least 10,000,000 EUR or up to 2% of the total worldwide annual turnover** of the undertaking to which the **ESSENTIAL ENTITY** belongs in the preceding financial year, whichever is higher.

A maximum of **at least 7,000,000 EUR or 1,4% of the total worldwide annual turnover of** the undertaking to which the **IMPORTANT ENTITY** belongs in the preceding financial year, whichever is higher.

NIS2 compliance

How to become compliant?

Essential Entities



Certification Cyber Fundamentals by an accredited CAB

(ESSENTIAL) or Label BASIC/IMPORTANT

OR

Certification ISO 27001 by an accredited CAB

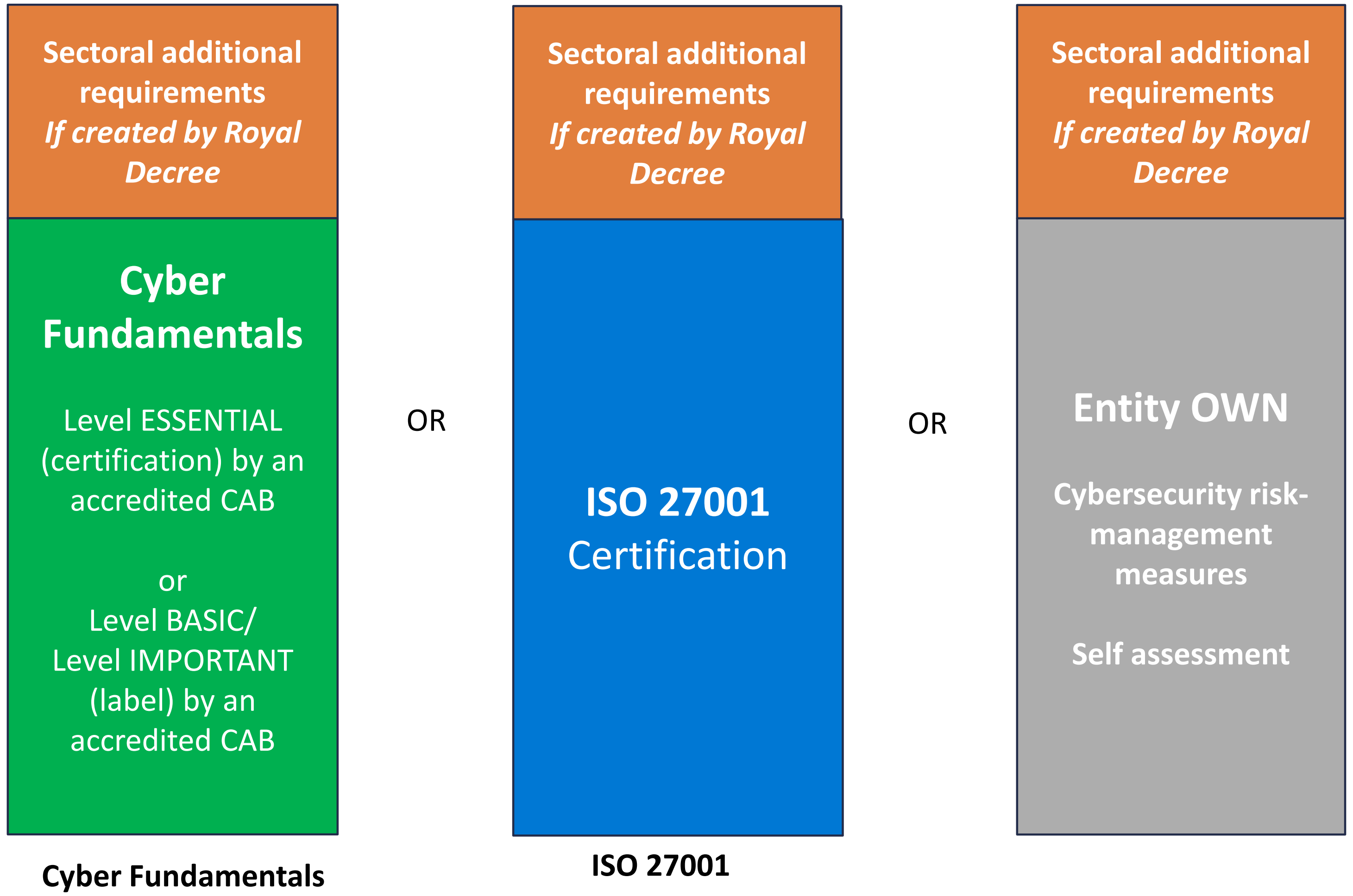
OR

Inspection by CCB

NIS2 Security measures (cost for the entity)

Presumption of conformity

Important Entities



Sectoral additional requirements
If created by Royal Decree

Cyber Fundamentals

Level ESSENTIAL (certification) by an accredited CAB

or

Level BASIC/ Level IMPORTANT (label) by an accredited CAB

Cyber Fundamentals

OR

Sectoral additional requirements
If created by Royal Decree

ISO 27001 Certification

ISO 27001

OR

Sectoral additional requirements
If created by Royal Decree

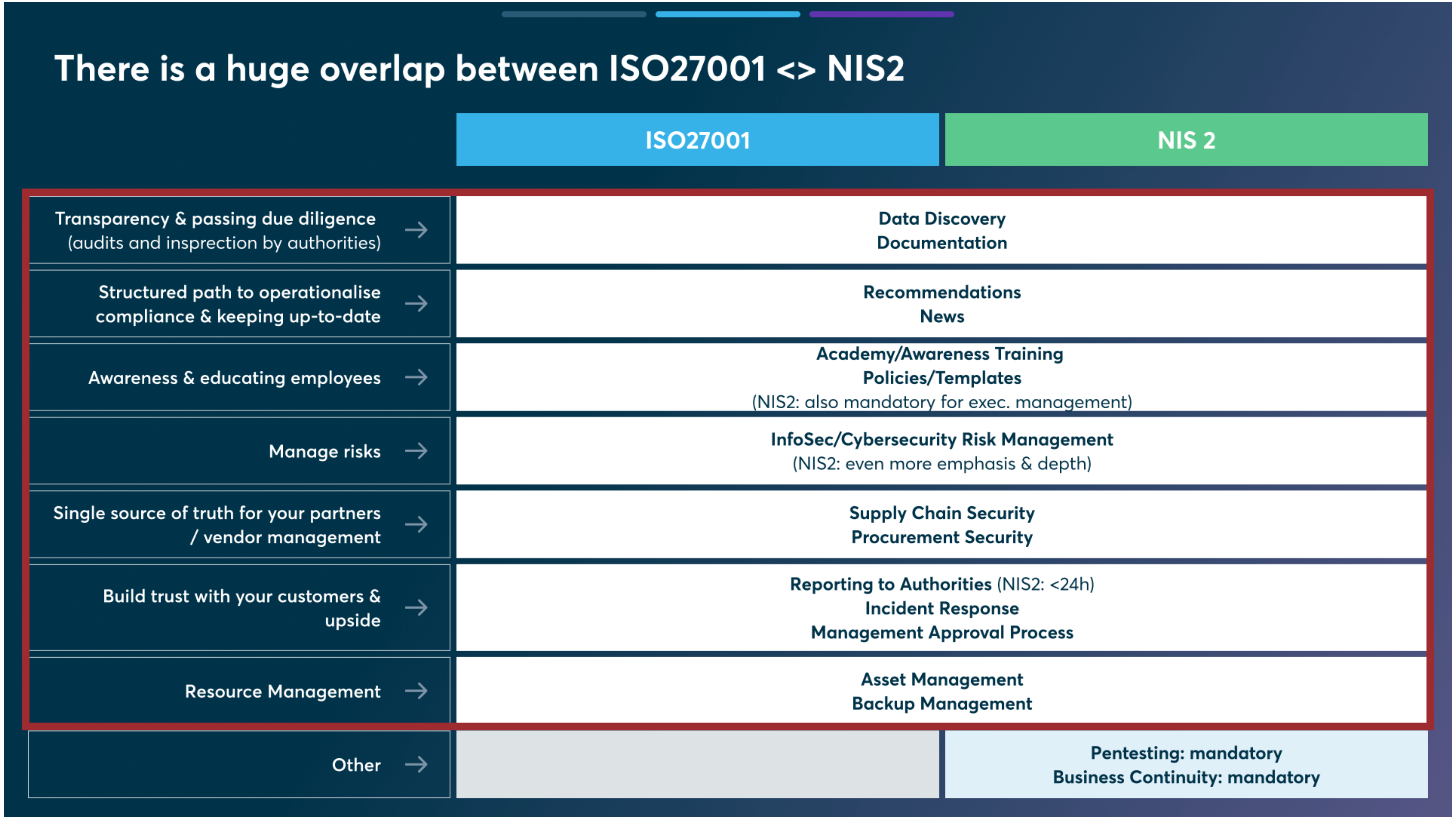
Entity OWN

Cybersecurity risk-management measures

Self assessment

NIS2 compliance

How to become compliant?



There is a huge overlap between ISO27001 <> NIS2

	ISO27001	NIS 2
Transparency & passing due diligence (audits and inspection by authorities) →	**Data Discovery** **Documentation**	
Structured path to operationalise compliance & keeping up-to-date →	**Recommendations** **News**	
Awareness & educating employees →	**Academy/Awareness Training** **Policies/Templates** (NIS2: also mandatory for exec. management)	
Manage risks →	**InfoSec/Cybersecurity Risk Management** (NIS2: even more emphasis & depth)	
Single source of truth for your partners / vendor management →	**Supply Chain Security** **Procurement Security**	
Build trust with your customers & upside →	**Reporting to Authorities** (NIS2: <24h) **Incident Response** **Management Approval Process**	
Resource Management →	**Asset Management** **Backup Management**	
Other →		**Pentesting: mandatory** **Business Continuity: mandatory**

Step by step guide

1. Determine

If your business is impacted by NIS2.

Identify whether your company is included in the sectors defined by NIS2.

2. Awareness

Raise awareness of NIS2 requirements and penalties.

To ensure compliance, NIS2 sets out multiple types of sanctions that must be raised to management.

3. Educate

And train management about cybersecurity risk management.

Ensure your top management is familiar with cybersecurity risks and how to manage them.

4. Plan

And budget for the increase in expenditures.

Estimate the expenses associated with NIS2 compliance.

5. Review

The ten cybersecurity risk management measures mandated by NIS2.

Evaluate how well your current cybersecurity policies and procedures align with these measures.

Step by step guide

6. Implement

Appropriate and proportional technical, operational and organizational measures to manage the risks posed to the systems.

7. Supply chain

Assess your supply chain security.

Evaluate your supply chain's cybersecurity risks. Ensure that suppliers comply with NIS2 standards.

8. Reporting

Simplify incident reporting.

Streamline your incident response reporting procedures to comply with NIS2 standards.

9. Continuity

Develop a business continuity and crisis management plan.

Create a business continuity plan that addresses NIS2 compliance.

10. ISMS

Implement an ISMS taking into account NIS2 criteria.

Ensure that the ISMS is appropriately implemented across your organization.

Cybersecurity Accelerator Program

Identify & Inspire

Audit & Assessment
Ethical hacking
Roadmap
Proof of Concept

Protect & Integrate

Zero Trust implementation

- Identities
- Devices
- Data
- Applications
- Networks & Infrastructure

Detect & Operate

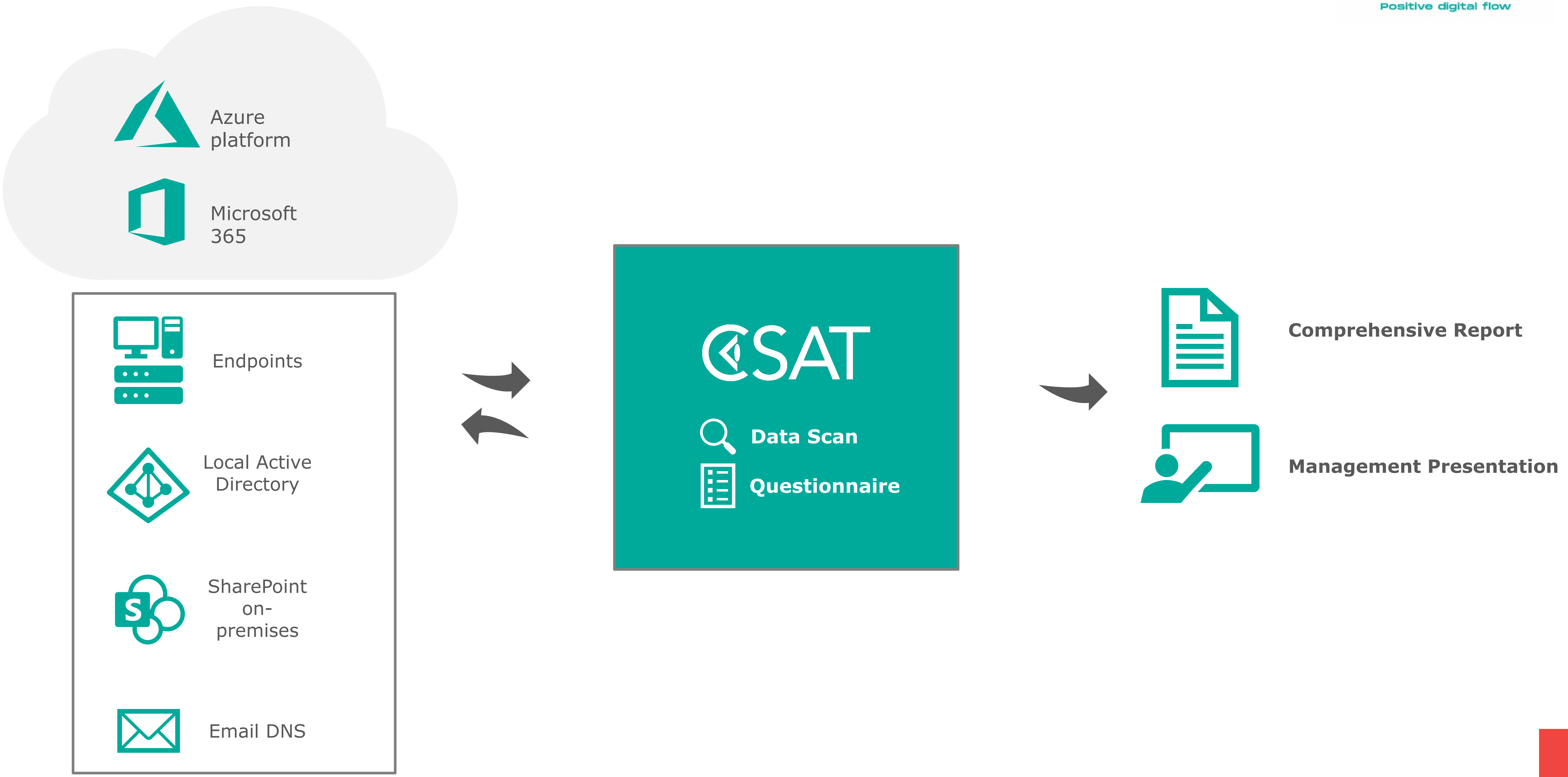
Managed Security Services
Vulnerability Management
SIEM & SOC Services

Respond & Optimize

Incident Response
Governance
CISO as a Service

▶

CSAT Data Collection



Azure platform

Microsoft 365

Endpoints

Local Active Directory

SharePoint on-premises

Email DNS

CSAT

Data Scan

Questionnaire

Comprehensive Report

Management Presentation

Steps of the Cybersecurity Assessment

Step 1

Let's get **started**!

Set-up a kick-off call with a Cybersecurity specialist to:

- Make introductions
- Discuss goals of the assessment
- Share system requirements

Prepare your environment for the assessment and plan next activities

Step 2

We **collect and analyze** your IT asset data

One of our Cybersecurity specialists runs the scans & tests to collect relevant data

Discuss your organization's cybersecurity posture in an interview (IT manager/CIO/CISO required)

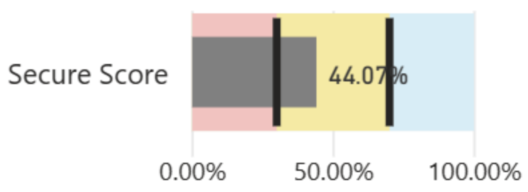
Step 3

Presentation of the report

Deliver presentation and discuss findings, conclusions and recommendations.

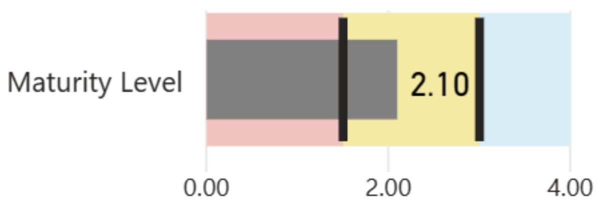
Share final report and presentation

ENVIRONMENT



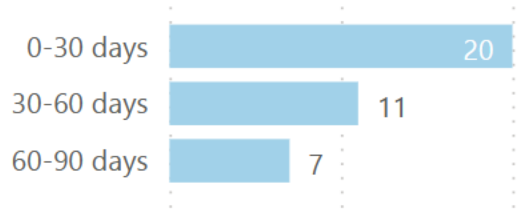
CIS MATURITY LEVEL

CIS v8 Average Maturity Level



APPROACH PLAN

Approach Plan Period



Cloud: Azure Discovery

Azure Accounts Provides a snapshot summary of Azure AD accounts (internal and external users).

On Premise: Active Directory

AD Accounts Provides a snapshot summary of on-premises AD accounts.

AD Groups Overviews membership to on-premises AD groups as well as AD password policies.

AD Devices Review the computer accounts in your organizational Active Directory

Cloud: Microsoft 365

Licenses Understand your current licensing position and review your enabled assets

Microsoft 365 MFA Presents the MFA status on Azure AD accounts.

Secure Score A measurement of your organization's security posture, recommendations based on system configurations and user behaviour, across M365 services.

On-Premise: Endpoints

1 2

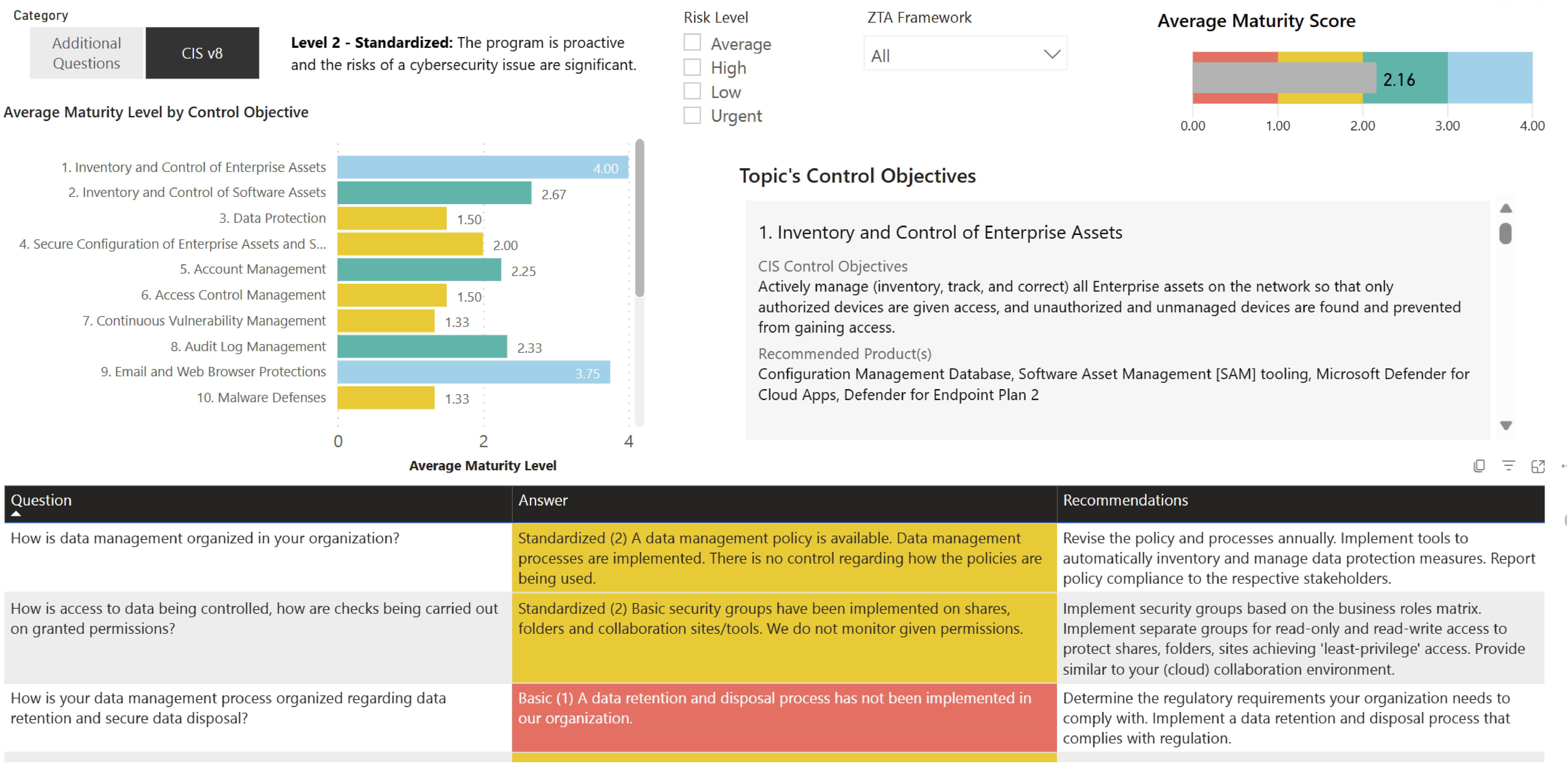
Endpoint Analysis Provides a snapshot of risks associated to endpoints (client and server) including out of support Operating Systems.

Applications Provides a repository of software installs and brings vulnerable installations to the forefront.

Missing Updates Assesses the types of updates that are missing from Windows systems.

SQL Instances Presents the support status of SQL instances.

Analysis Shares Discover directories that are currently accessible to multiple users on a network.


Category
Additional Questions
CIS v8
Risk Level
☐ Average
☐ High
☐ Low
☐ Urgent
ZTA Framework
All
Average Maturity Score
2.16
0.00
1.00
2.00
3.00
4.00
Average Maturity Level by Control Objective
1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and S...
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser Protections
10. Malware Defenses
4.00
2.67
1.50
2.00
2.25
1.50
1.33
2.33
3.75
1.33
0
2
4
Average Maturity Level

Level 2 - Standardized: The program is proactive and the risks of a cybersecurity issue are significant.

Topic's Control Objectives

1. Inventory and Control of Enterprise Assets

CIS Control Objectives

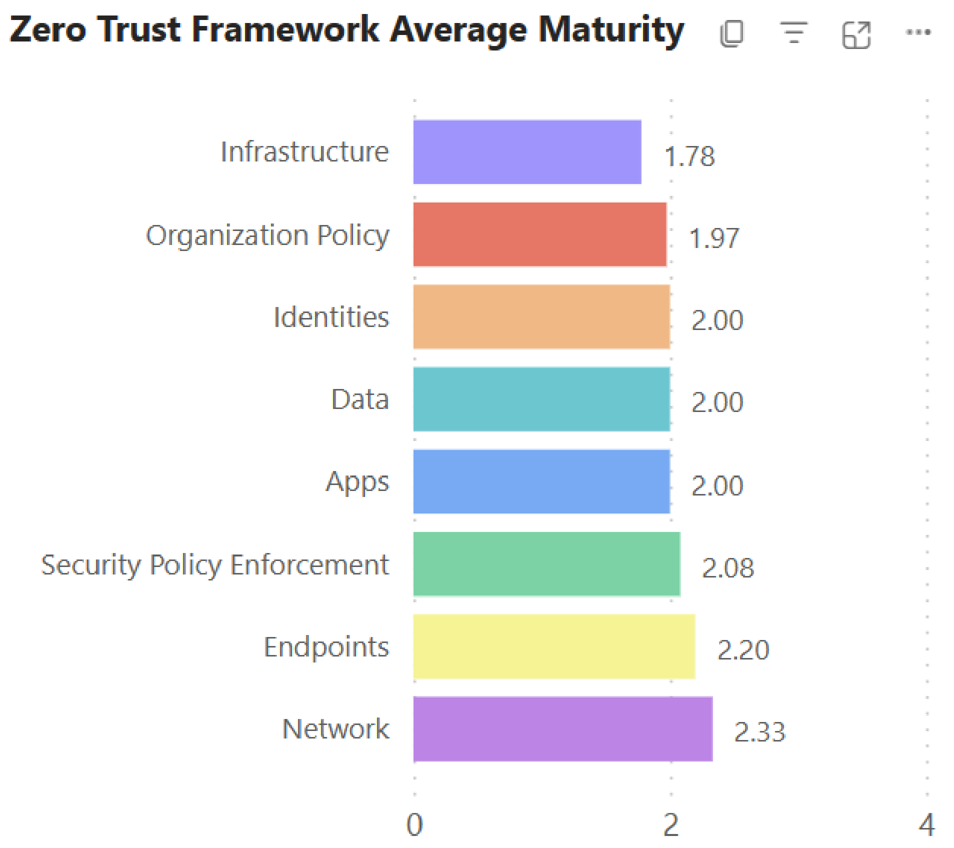
Actively manage (inventory, track, and correct) all Enterprise assets on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

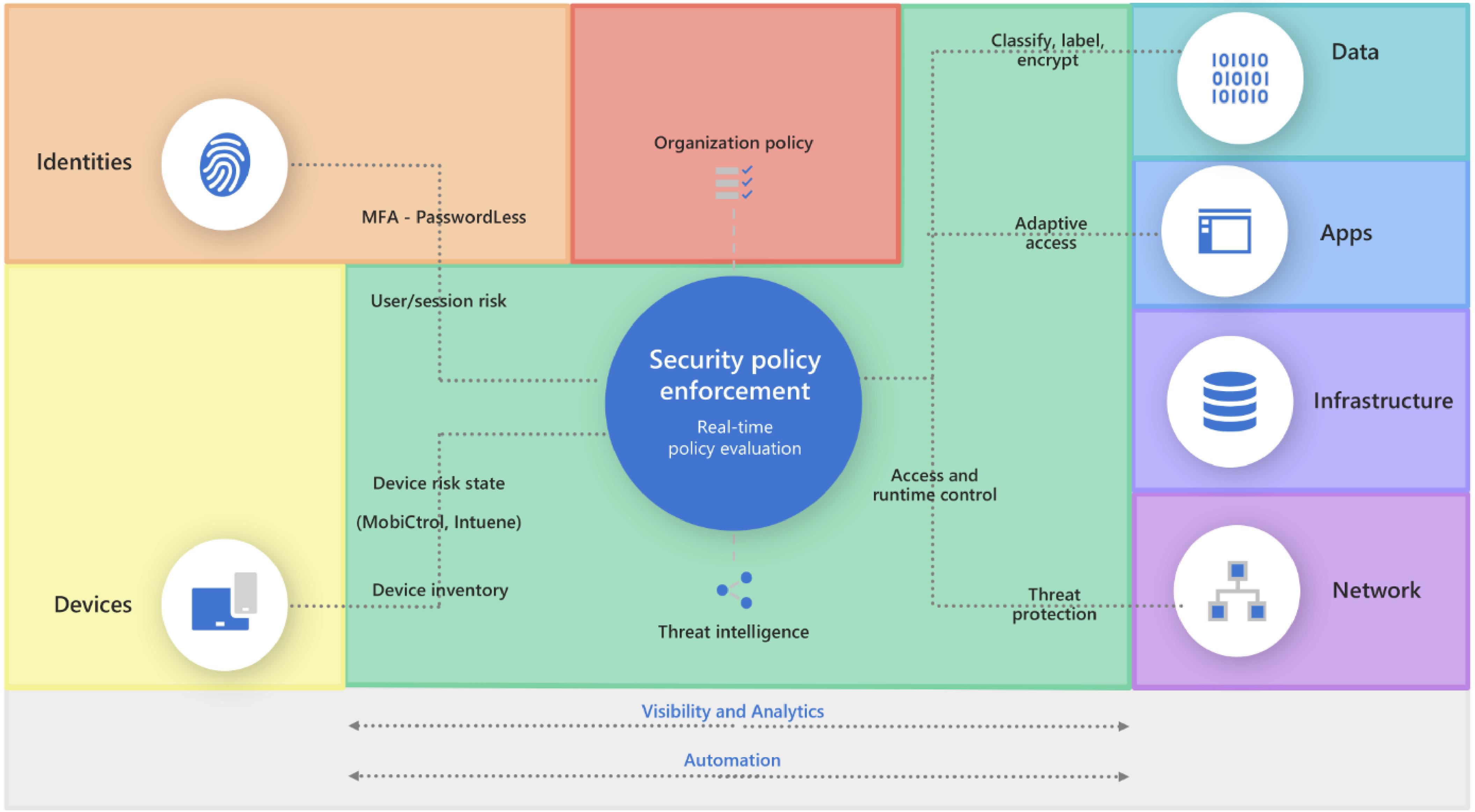
Recommended Product(s)

Configuration Management Database, Software Asset Management [SAM] tooling, Microsoft Defender for Cloud Apps, Defender for Endpoint Plan 2

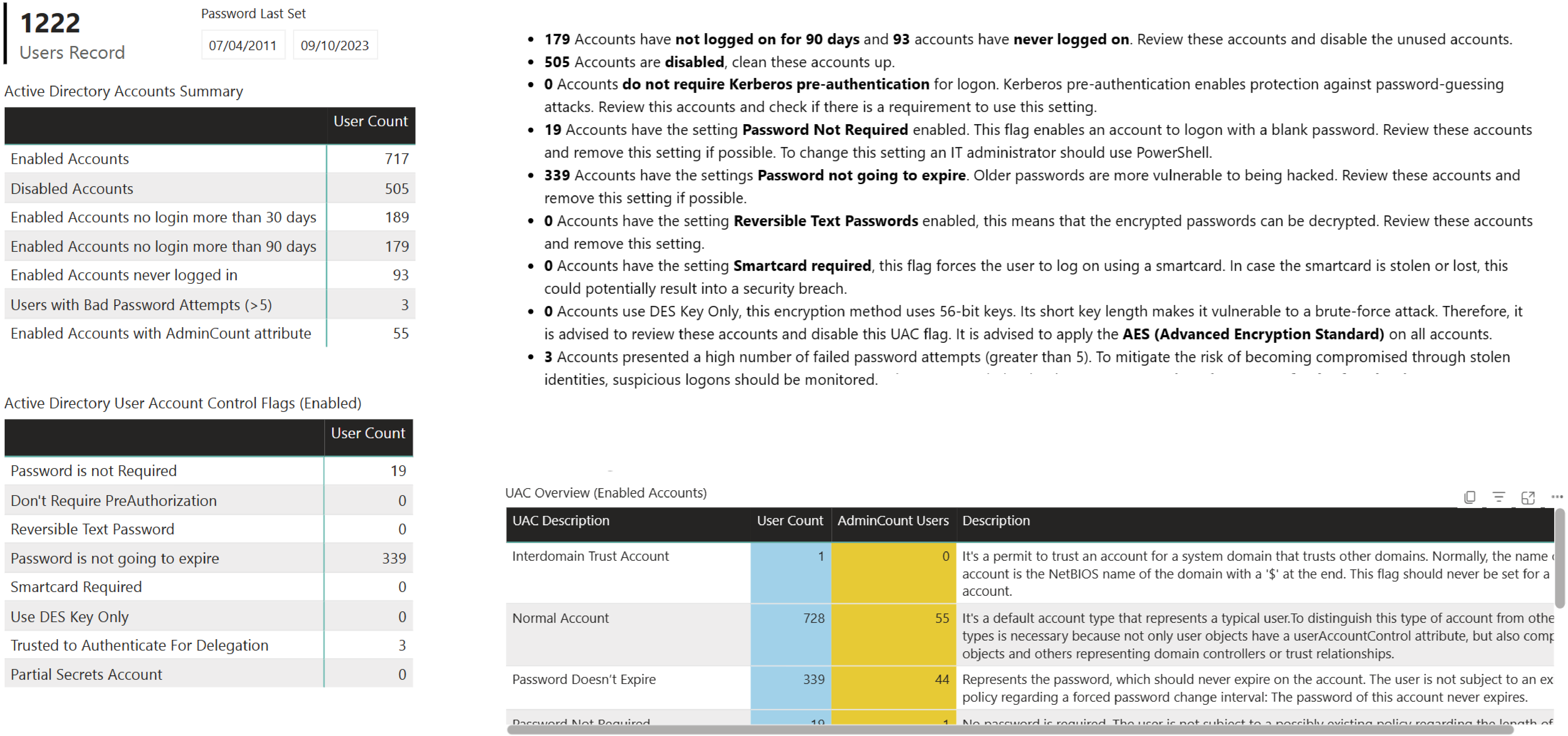
Question	Answer	Recommendations
How is data management organized in your organization?	Standardized (2) A data management policy is available. Data management processes are implemented. There is no control regarding how the policies are being used.	Revise the policy and processes annually. Implement tools to automatically inventory and manage data protection measures. Report policy compliance to the respective stakeholders.
How is access to data being controlled, how are checks being carried out on granted permissions?	Standardized (2) Basic security groups have been implemented on shares, folders and collaboration sites/tools. We do not monitor given permissions.	Implement security groups based on the business roles matrix. Implement separate groups for read-only and read-write access to protect shares, folders, sites achieving 'least-privilege' access. Provide similar to your (cloud) collaboration environment.
How is your data management process organized regarding data retention and secure data disposal?	Basic (1) A data retention and disposal process has not been implemented in our organization.	Determine the regulatory requirements your organization needs to comply with. Implement a data retention and disposal process that complies with regulation.

***Zero-Trust Architecture** is an enterprise's cybersecurity plan that utilizes zero-trust concepts and encompasses component relationships, workflow planning, and access policies.*


Zero Trust Framework Average Maturity



ZTA Framework	Recommendation
Organization Policy	Configure a single central authentication source for all applications and systems, cloud as well as on-premises.
Organization Policy	Create a data classification scheme and create the corresponding labels. Instruct users in how to use the labels in order to comply with regulatory requirements.
Organization Policy	Create a process to document the given access, assessment on security measures, monitoring, and decommissioning of the service providers.
Organization Policy	Designate a key resource(s) to handle the reported security incidents.



1222

Users Record

Password Last Set

07/04/2011 | 09/10/2023

Active Directory Accounts Summary

	User Count
Enabled Accounts	717
Disabled Accounts	505
Enabled Accounts no login more than 30 days	189
Enabled Accounts no login more than 90 days	179
Enabled Accounts never logged in	93
Users with Bad Password Attempts (>5)	3
Enabled Accounts with AdminCount attribute	55

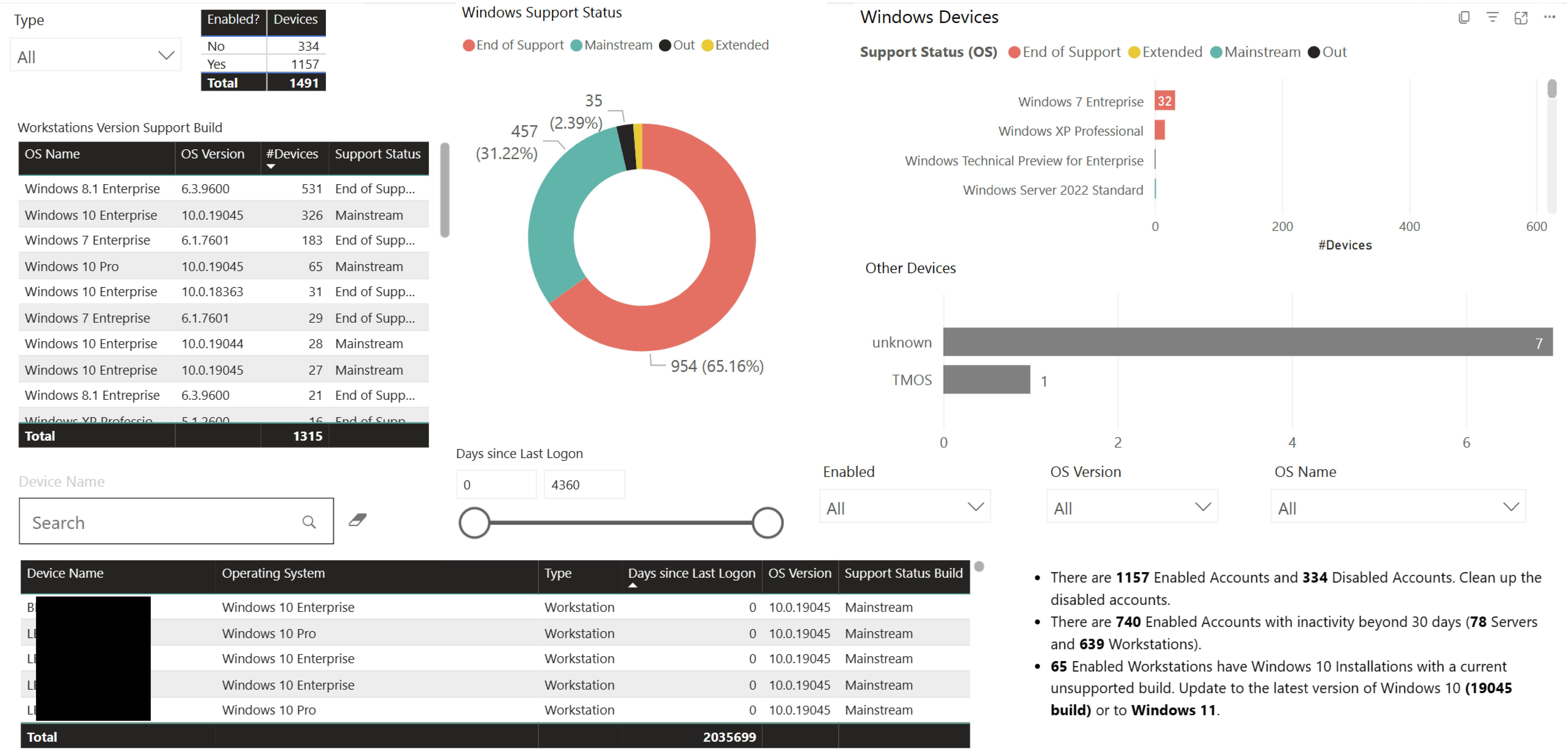
Active Directory User Account Control Flags (Enabled)

	User Count
Password is not Required	19
Don't Require PreAuthorization	0
Reversible Text Password	0
Password is not going to expire	339
Smartcard Required	0
Use DES Key Only	0
Trusted to Authenticate For Delegation	3
Partial Secrets Account	0

- **179** Accounts have **not logged on for 90 days** and **93** accounts have **never logged on**. Review these accounts and disable the unused accounts.
- **505** Accounts are **disabled**, clean these accounts up.
- **0** Accounts **do not require Kerberos pre-authentication** for logon. Kerberos pre-authentication enables protection against password-guessing attacks. Review this accounts and check if there is a requirement to use this setting.
- **19** Accounts have the setting **Password Not Required** enabled. This flag enables an account to logon with a blank password. Review these accounts and remove this setting if possible. To change this setting an IT administrator should use PowerShell.
- **339** Accounts have the settings **Password not going to expire**. Older passwords are more vulnerable to being hacked. Review these accounts and remove this setting if possible.
- **0** Accounts have the setting **Reversible Text Passwords** enabled, this means that the encrypted passwords can be decrypted. Review these accounts and remove this setting.
- **0** Accounts have the setting **Smartcard required**, this flag forces the user to log on using a smartcard. In case the smartcard is stolen or lost, this could potentially result into a security breach.
- **0** Accounts use DES Key Only, this encryption method uses 56-bit keys. Its short key length makes it vulnerable to a brute-force attack. Therefore, it is advised to review these accounts and disable this UAC flag. It is advised to apply the **AES (Advanced Encryption Standard)** on all accounts.
- **3** Accounts presented a high number of failed password attempts (greater than 5). To mitigate the risk of becoming compromised through stolen identities, suspicious logons should be monitored.

UAC Overview (Enabled Accounts)

UAC Description	User Count	AdminCount Users	Description
Interdomain Trust Account	1	0	It's a permit to trust an account for a system domain that trusts other domains. Normally, the name account is the NetBIOS name of the domain with a '$' at the end. This flag should never be set for a account.
Normal Account	728	55	It's a default account type that represents a typical user.To distinguish this type of account from othe types is necessary because not only user objects have a userAccountControl attribute, but also comp objects and others representing domain controllers or trust relationships.
Password Doesn't Expire	339	44	Represents the password, which should never expire on the account. The user is not subject to an ex policy regarding a forced password change interval: The password of this account never expires.
Password Not Required	19	1	No password is required. The user is not subject to a possibly existing policy regarding the length of



Type

All

Enabled?	Devices
No	334
Yes	1157
Total	**1491**

Workstations Version Support Build

OS Name	OS Version	#Devices	Support Status
Windows 8.1 Enterprise	6.3.9600	531	End of Supp...
Windows 10 Enterprise	10.0.19045	326	Mainstream
Windows 7 Enterprise	6.1.7601	183	End of Supp...
Windows 10 Pro	10.0.19045	65	Mainstream
Windows 10 Enterprise	10.0.18363	31	End of Supp...
Windows 7 Entreprise	6.1.7601	29	End of Supp...
Windows 10 Enterprise	10.0.19044	28	Mainstream
Windows 10 Entreprise	10.0.19045	27	Mainstream
Windows 8.1 Entreprise	6.3.9600	21	End of Supp...
Windows XP Professio...	5.1.2600	16	End of Supp...
Total		**1315**	

Windows Support Status

Windows Devices

Support Status (OS) ● End of Support ● Extended ● Mainstream ● Out
Windows 7 Entreprise
32
Windows XP Professional
Windows Technical Preview for Enterprise
Windows Server 2022 Standard
0
200
400
600
#Devices

Other Devices

Days since Last Logon

0 4360

Enabled

All

OS Version

All

OS Name

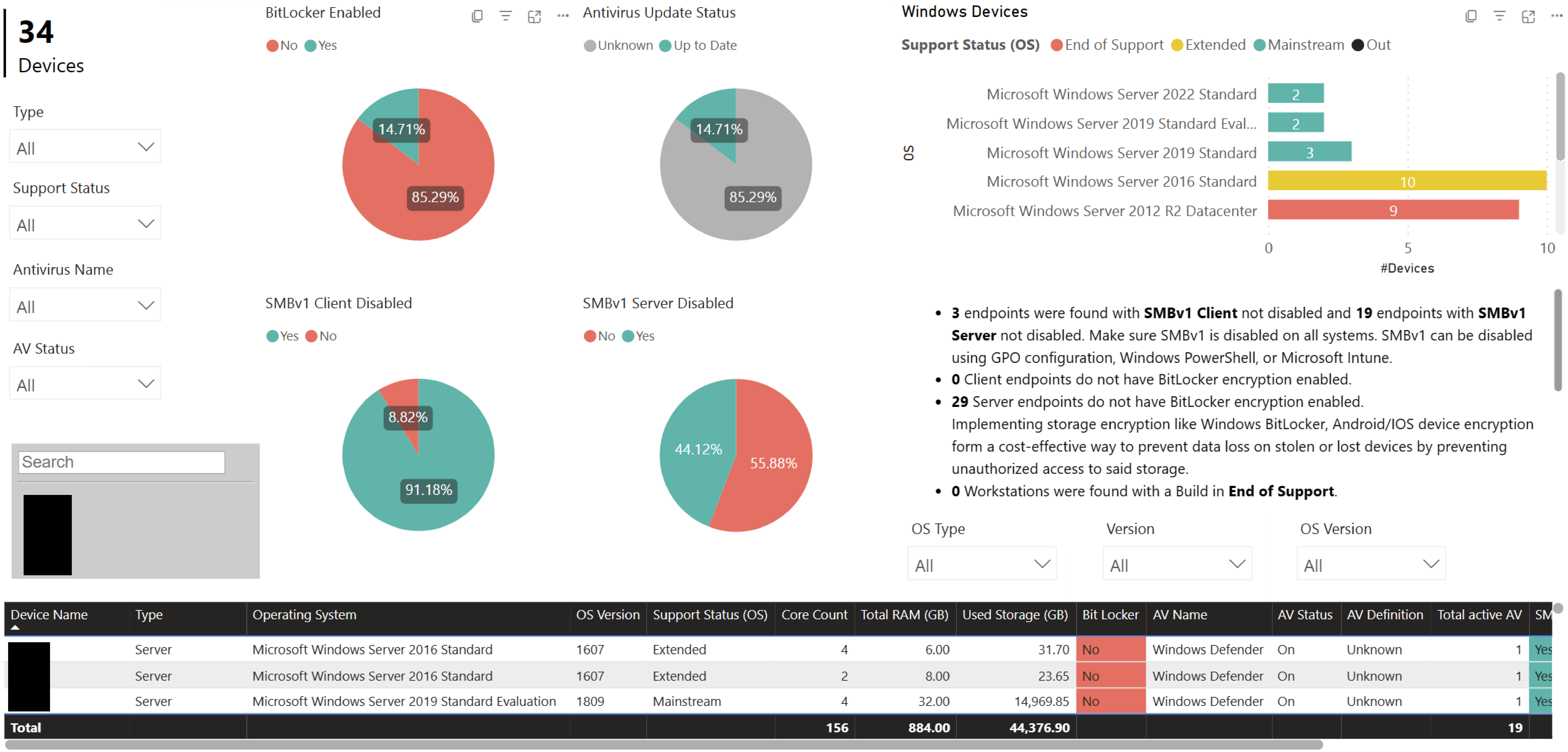
All

Device Name

Search

Device Name	Operating System	Type	Days since Last Logon	OS Version	Support Status Build
[redacted]	Windows 10 Enterprise	Workstation	0	10.0.19045	Mainstream
[redacted]	Windows 10 Pro	Workstation	0	10.0.19045	Mainstream
[redacted]	Windows 10 Enterprise	Workstation	0	10.0.19045	Mainstream
[redacted]	Windows 10 Enterprise	Workstation	0	10.0.19045	Mainstream
[redacted]	Windows 10 Pro	Workstation	0	10.0.19045	Mainstream
Total			**2035699**		

- There are **1157** Enabled Accounts and **334** Disabled Accounts. Clean up the disabled accounts.
- There are **740** Enabled Accounts with inactivity beyond 30 days (**78** Servers and **639** Workstations).
- **65** Enabled Workstations have Windows 10 Installations with a current unsupported build. Update to the latest version of Windows 10 **(19045 build)** or to **Windows 11**.



BitLocker Enabled
● No ● Yes
14.71%
85.29%
Antivirus Update Status
● Unknown ● Up to Date
14.71%
85.29%
SMBv1 Client Disabled
● Yes ● No
8.82%
91.18%
SMBv1 Server Disabled
● No ● Yes
44.12%
55.88%
Windows Devices
Support Status (OS) ● End of Support ● Extended ● Mainstream ● Out
OS
Microsoft Windows Server 2022 Standard
2
Microsoft Windows Server 2019 Standard Eval...
2
Microsoft Windows Server 2019 Standard
3
Microsoft Windows Server 2016 Standard
10
Microsoft Windows Server 2012 R2 Datacenter
9
0
5
10
#Devices

34

Devices

Type: All

Support Status: All

Antivirus Name: All

AV Status: All

Search

[redacted]

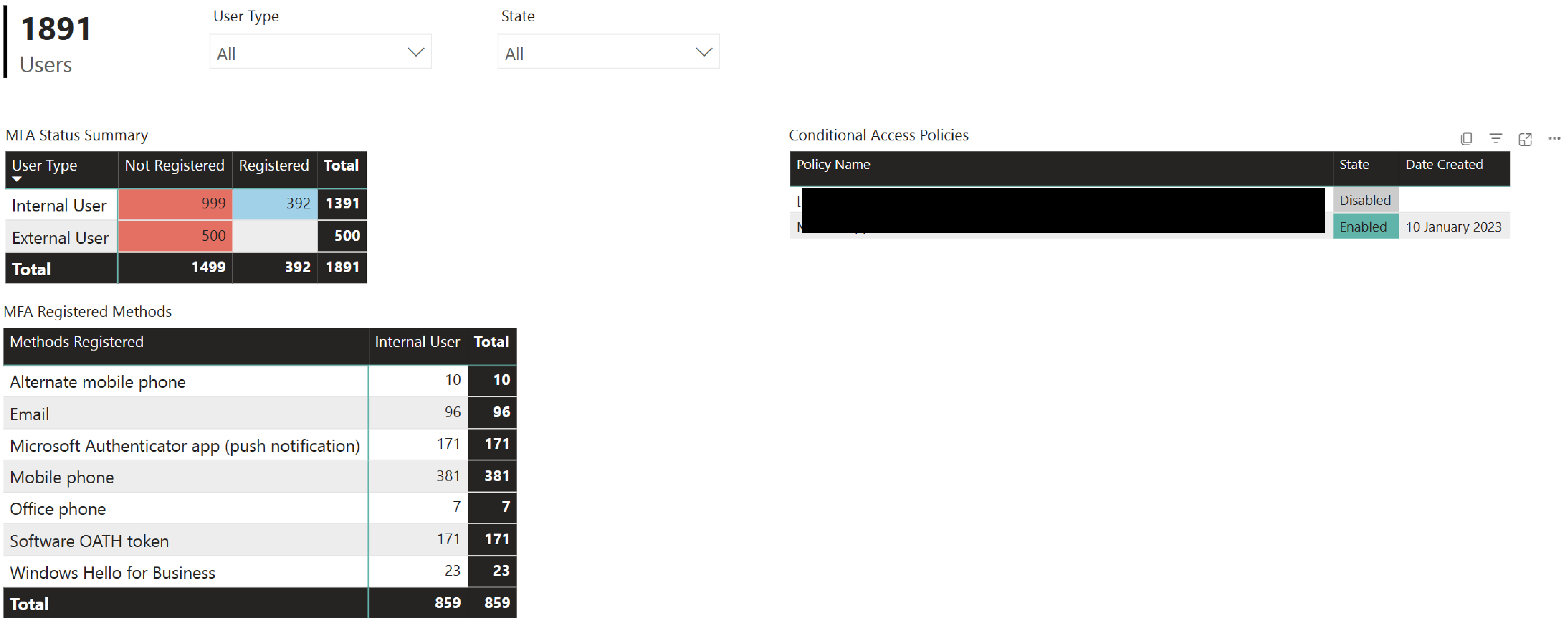
- **3** endpoints were found with **SMBv1 Client** not disabled and **19** endpoints with **SMBv1 Server** not disabled. Make sure SMBv1 is disabled on all systems. SMBv1 can be disabled using GPO configuration, Windows PowerShell, or Microsoft Intune.
- **0** Client endpoints do not have BitLocker encryption enabled.
- **29** Server endpoints do not have BitLocker encryption enabled. Implementing storage encryption like Windows BitLocker, Android/IOS device encryption form a cost-effective way to prevent data loss on stolen or lost devices by preventing unauthorized access to said storage.
- **0** Workstations were found with a Build in **End of Support**.

OS Type: All

Version: All

OS Version: All

Device Name	Type	Operating System	OS Version	Support Status (OS)	Core Count	Total RAM (GB)	Used Storage (GB)	Bit Locker	AV Name	AV Status	AV Definition	Total active AV	SM
[redacted]	Server	Microsoft Windows Server 2016 Standard	1607	Extended	4	6.00	31.70	No	Windows Defender	On	Unknown	1	Yes
[redacted]	Server	Microsoft Windows Server 2016 Standard	1607	Extended	2	8.00	23.65	No	Windows Defender	On	Unknown	1	Yes
[redacted]	Server	Microsoft Windows Server 2019 Standard Evaluation	1809	Mainstream	4	32.00	14,969.85	No	Windows Defender	On	Unknown	1	Yes
Total					**156**	**884.00**	**44,376.90**					**19**	



1891

Users

User Type

All

State

All

MFA Status Summary

User Type	Not Registered	Registered	Total
Internal User	999	392	1391
External User	500		500
Total	1499	392	1891

Conditional Access Policies

Policy Name	State	Date Created
[redacted]	Disabled	
[redacted]	Enabled	10 January 2023

MFA Registered Methods

Methods Registered	Internal User	Total
Alternate mobile phone	10	10
Email	96	96
Microsoft Authenticator app (push notification)	171	171
Mobile phone	381	381
Office phone	7	7
Software OATH token	171	171
Windows Hello for Business	23	23
Total	859	859

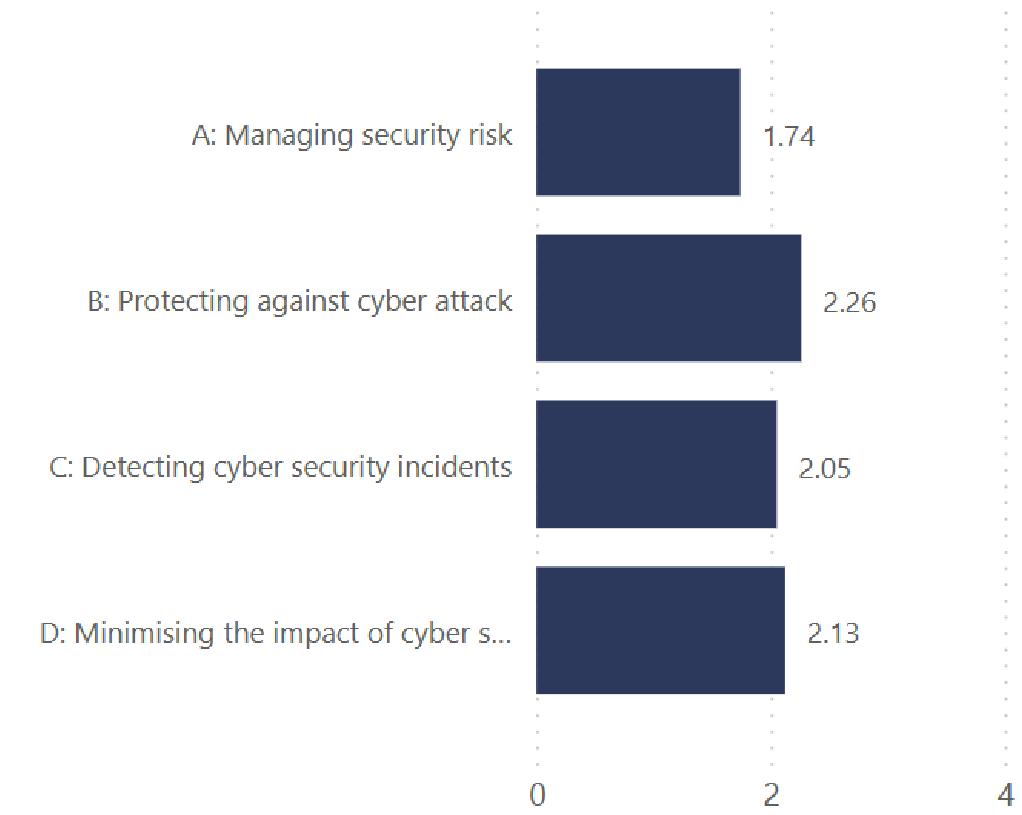
The **NIS 2 Directive** is the EU-wide legislation on cybersecurity. The goal of NIS 2 is to enhance the security level in the same level across the EU. Some of the key benefits of the NIS 2 Directive:

- Improve the cybersecurity posture of your businesses across EU, making it more resilient to cyberattacks.
- Promote a more harmonized approach to cybersecurity, making it easier for businesses to operate across borders.
- Strengthen the EU's ability to respond to cyberattacks and other cybersecurity threats.

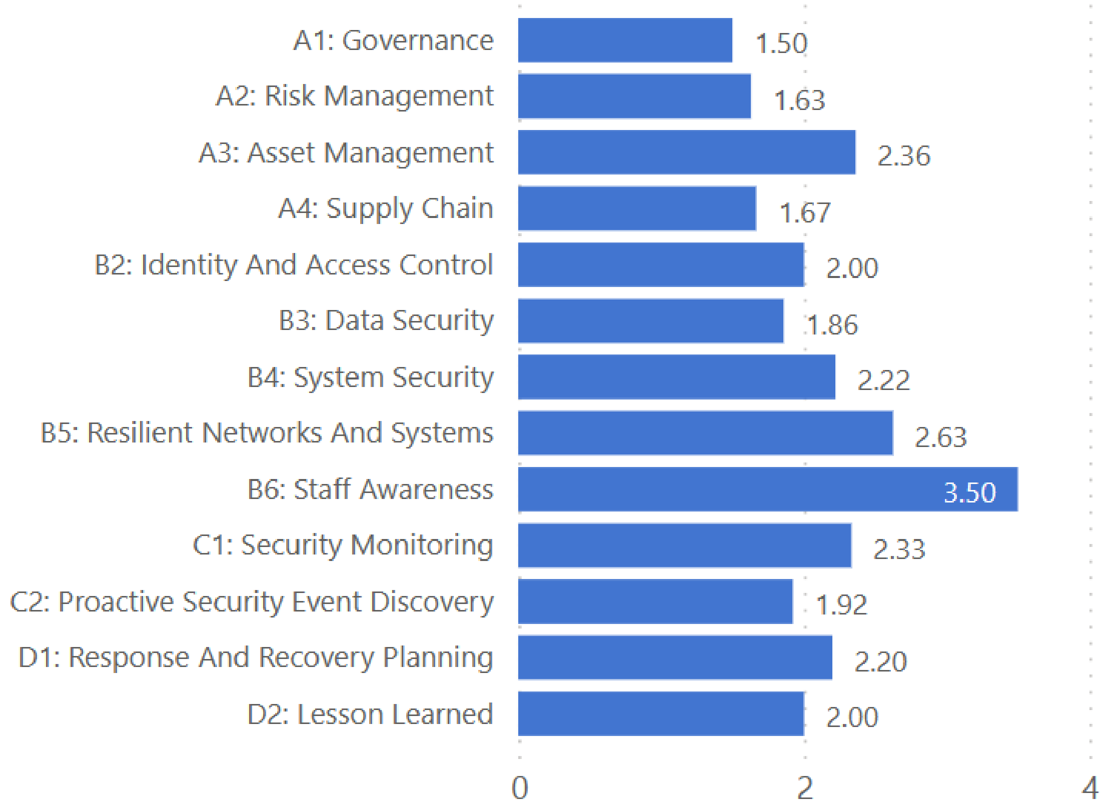
NIS 2 Principles have been linked with the questionnaire to provide a current state based on the **NIS Regulations - Compliance Framework** (some questions may apply to more than one Principle)

NIS2 Directive

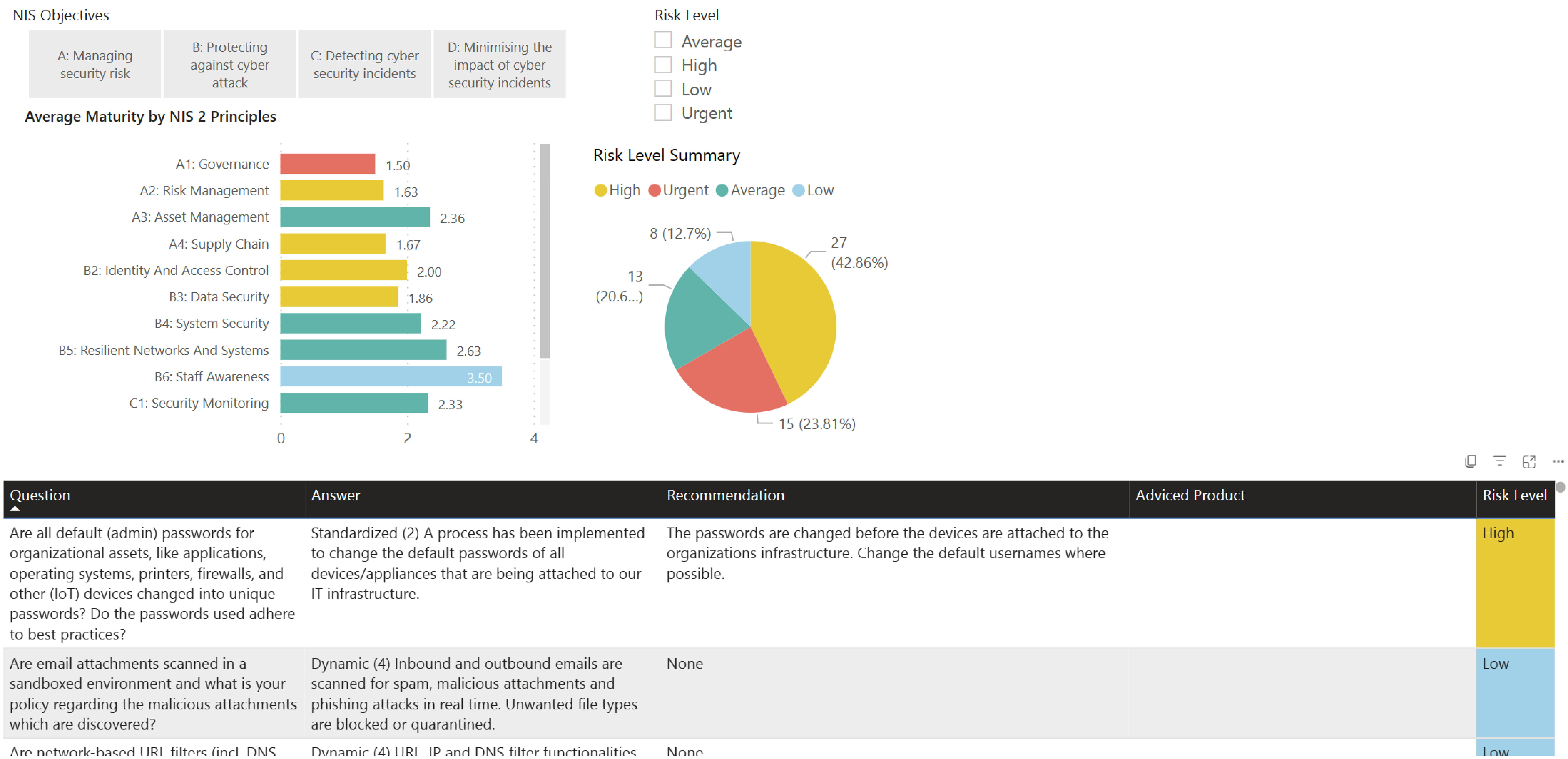
NIS 2 Objectives Average Maturity



NIS 2 Principles Average Maturity



Questionnaire



NIS Objectives

A: Managing security risk	B: Protecting against cyber attack	C: Detecting cyber security incidents	D: Minimising the impact of cyber security incidents

Risk Level

□ Average
□ High
□ Low
□ Urgent

Question	Answer	Recommendation	Adviced Product	Risk Level
Are all default (admin) passwords for organizational assets, like applications, operating systems, printers, firewalls, and other (IoT) devices changed into unique passwords? Do the passwords used adhere to best practices?	Standardized (2) A process has been implemented to change the default passwords of all devices/appliances that are being attached to our IT infrastructure.	The passwords are changed before the devices are attached to the organizations infrastructure. Change the default usernames where possible.		High
Are email attachments scanned in a sandboxed environment and what is your policy regarding the malicious attachments which are discovered?	Dynamic (4) Inbound and outbound emails are scanned for spam, malicious attachments and phishing attacks in real time. Unwanted file types are blocked or quarantined.	None		Low
Are network-based URL filters (incl. DNS	Dynamic (4) URL, IP and DNS filter functionalities	None		Low

First Phase

Second Phase

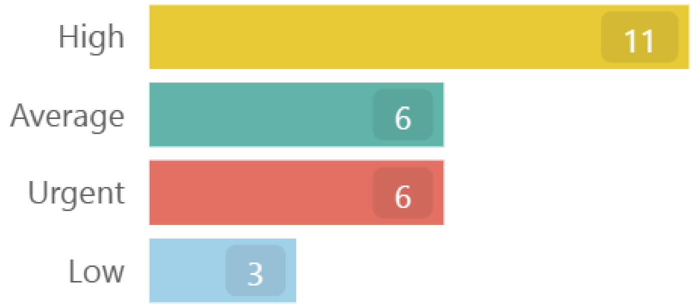
Third Phase

The information gathered during the interview with your security team, along with the technical facts gathered from the **CSAT scan**, result in **recommendations** to get on par with the current recommended practices. The multitude of them can be overwhelming. The below **plan of approach** is our suggestion on how to **prioritize** them.

The **First Phase** is focused to mitigate the risk against **rapid cyberattacks**, and to enable so-called **'low-hanging fruit'** features (features that are relatively easy to implement yet with high impact on preventing security incidents). It also focuses on **rejuvenating your security strategy.**

Human-Operated Ransomware	Topic	Category
All	All	All

Risk Level



Approach Plan: 0-30 Days

Topic	Recommendation	Recommended Product	Note	Risk Level
19. AQ 1. IT Governance	Establish an IT security plan or roadmap that covers all relevant business objectives, compliance requirements and risk mitigation plans	[redacted]	Roadmap is being defined	Urgent
20. AQ 2. Data Governance	Implement a basic risk management process.	[redacted]		Urgent
5. Account Management	Implement a process to check for dormant administrator, service and user accounts. Ensure the process is scheduled at least quarterly.	[redacted]		Urgent
6. Access Control Management	Implement business ownership of all accounts/identities, including checks by the business/functional owner of each accounts/identities. Cleanup old accounts/identities	[redacted]		Urgent
7. Continuous Vulnerability Management	Implement a basic risk assessment process.	[redacted]		Urgent
7. Continuous Vulnerability Management	Implement a process to identify or remediate software or configuration vulnerabilities. And perform this process on a quarterly, or more frequent, basis.	[redacted]		Urgent

Policies and Procedures

Option 1: - MVP Approach - CYFUN Belgium Alignment

1. Information Security Policy
2. Access Control Policy
3. Incident Response Policy
4. Data Classification and Handling Policy
5. Acceptable Use policy
6. Physical Security Policy
7. Business Continuity Plan
8. Disaster Recovery Policy
9. Asset Management Policy
10. Vendor Management Policy
11. Risk Assessment and Management Policy
12. Network Security Policy
13. Application Security Policy
14. Cryptography Policy
15. Employee Training and Awareness Policy
16. Endpoint Security Policy
17. Cloud Security Policy
18. Monitoring and Logging Policy

Option 2: - MVP Approach –Alignment with ISO27k1 & NIS2 Considerations

Option 1 + 7 more specific policies (25 total)

Option 3: - Comprehensive Approach – Full ISO27k1 and NIS2 Alignment

Option 2 + 9 more specific policies (34 total)

26. Physical and Environmental Security Policy
27. Communications Security Policy
28. Operations Security Policy
29. Security in Development and Support Processes Policy
30. Privacy and Protection of Personally Identifiable Information Policy
31. Security Policy for Mobile Devices and Teleworking
32. Secure Disposal or Re-use of Equipment Policy
33. Information Transfer Policy
34. Third party Management Policy

NIS2 Measures

All measures must be proportionate to risk, size, cost, and impact & severity of incidents. Take into account the state-of-the-art, and where applicable relevant European and international standards.

- Risk Analysis & Management
- Security Policies & Asset Management
- Incident Handling
- Business continuity and crisis management
- Supply chain security
- Vulnerability Management and Handling
- Regular assessments
- The use of encryption where appropriate
- Basic cybersecurity hygiene & training
- The use of MFA or continuous authentication

How Inetum-Realdolmen can help

At Inetum-Realdolmen, we understand the importance of cybersecurity and the need to comply with regulatory frameworks such as NIS2

We provide tools and guidance to help you meet the minimum measures required by NIS2, such as risk assessments, security procedures, and incident response plans

Our team of cybersecurity experts can work with you to assess your current security posture and develop a customized security plan that meets your specific needs

You can have peace of mind knowing that your systems and data are protected by industry-leading security solutions.