Interplay between NIS and GDPR in Cybersecurity

WELCOME to

ISACA Belgium Chapter & dpo pro Event

WWW.ISACA.BE

For public use.

CYBER SECURITY COALITION.be

dpo pro

ISACA Belgium Chapter

What Are We Talking About Today?

Interplay between NIS and GDPR in Cybersecurity

How to ensure an integrated implementation of cybersecurity in compliance with all regulatory requirements, namely NIS and GDPR?

***THANK YOU TO OUR SPEAKERS** GUEST:*

Mr **Benjamin Docquir** from Osborne Clarke,
Mr **Patrick Soenen** from dpo pro,
Mr **Stephan Van Dyck** from ISACA

THANK YOU TO P&V TO HOST THIS EVENT

ISACA
Belgium Chapter

JOIN ISACA BE & GET CERTIFIED

- A strong network of local IS/IT professionals in Belgium.
- Success in IS/IT audit, risk, control, security, cybersecurity and governance across a multitude of industries.
- Industry leading global conferences offering professional networking and education locally and globally.
- SheLeads Tech promoting women in leadership roles in technology.
- Access to the updated frameworks, publications and research of ISACA.
- Mentorship Programs & connection with other ISACA members for career development and support.

OUR CERTIFICATIONS :

CISA Certified Information Systems Auditor. An ISACA Certification

CISM Certified Information Systems Manager. An ISACA Certification

CSX-P CSX Cybersecurity Practitioner. An ISACA Certification

CGEIT Certified in the Governance of Enterprise IT. An ISACA Certification

CDPSE Certified Data Privacy Solutions Engineer. An ISACA Certification

CRISC Certified in Risk and Information Systems Control. An ISACA Certification

Governance Cybersecurity Privacy Enterprise Solutions IT Audit GDPR Emerging Tech Risk

Meeting Etiquette

- **CPE Participation**
  - The earned CPE will automatically appear in the **ISACA CPE RECORDS** tab ➔ on the **MyISACA** page ➔ in your ISACA account.
- **Q&A:**

The ISACA Belgium will monitor and moderate the discussion in the Q&A window and the Chat window.

- The presenters will review and answer the questions as time permits at the end.
- **Disclaimer** – This webinar will be recorded and shared with ISACA members & DPO PRO members only.
- **Feedback & Suggestions:** education@isaca.be

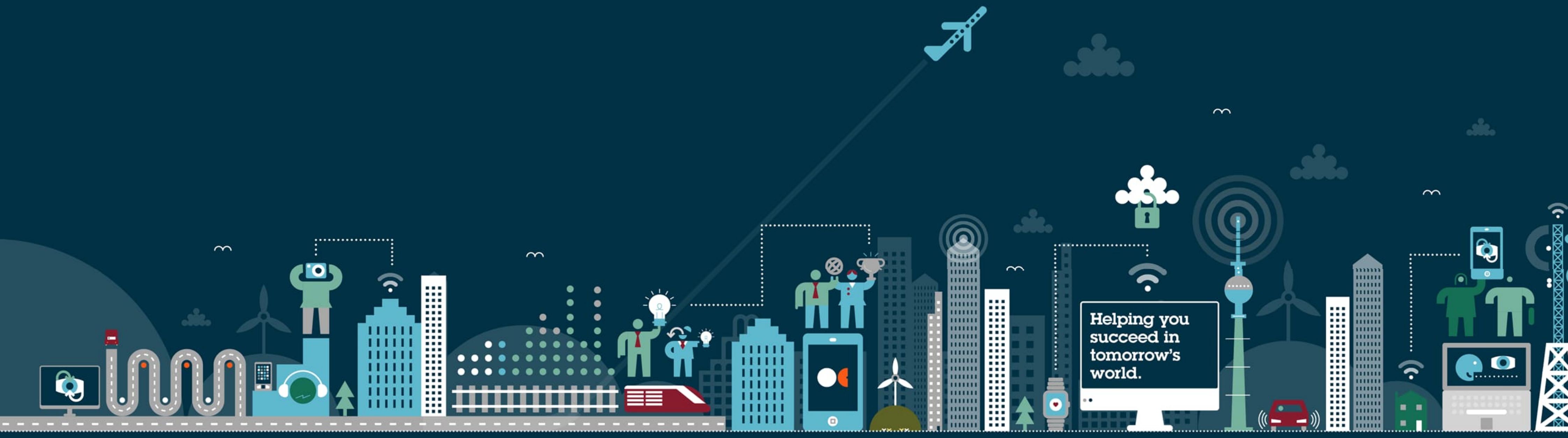
ISACA®
Belgium Chapter

Interplay between NIS and GDPR in Cybersecurity

NIS & GDPR Security Obligations: Can Common Sense Prevail?

Approach and key obligations

ISACA – DPOPro – 22 November 2022



Contents

01 Security as a Concept

02 Data Breaches

03 Q&A

01 Security as a Concept

"Classical" Belgian context

No harmonized regulatory framework to security

- Data Protection
- Electronic communications (confidentiality / integrity)
- Critical infrastructures
- Cybercrime (approaches authenticity, integrity, confidentiality of IT systems)
- Sectoral regulation

General rules in civil law

- Code civil "bonus pater familias" v. protection of the information
- Partial insurance coverage based on "breaches" (but what is a breach?)

Contractual approach

- Rules of the art, highest standards, etc.
- SLA's
- Access controls, confidentiality & NDA's, Key Personnel, etc.

Major changes brought about by the GDPR

Duties of Data Processors

- Transparency & limited accountability (register, DPO, etc.)
- Confidentiality & Purpose Limitation
- Security & access rules set forth in a written contract
- Data transfers outside EU/EEA

Duties of Data Controllers

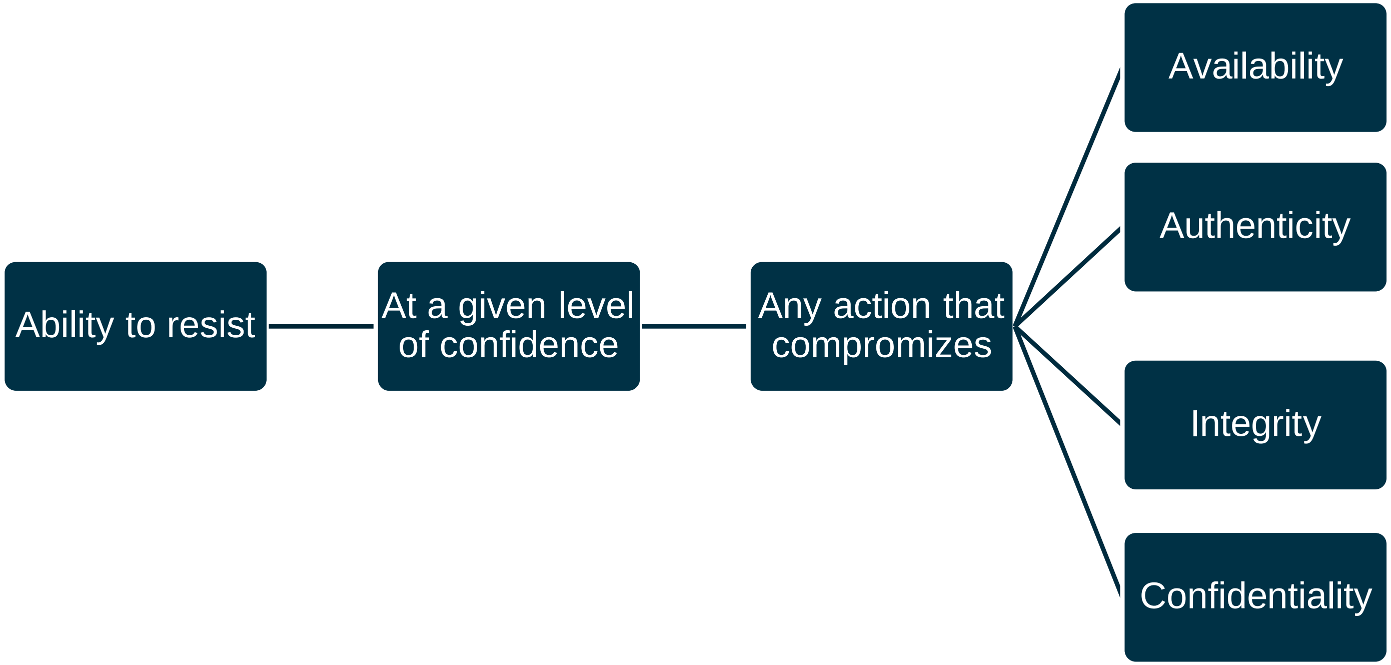
- Proportionality & Storage Limitation
- Notification of Data Breaches
- DPIAs

Technical & Organizational Measures (TOM's)

- Appropriate to the risk & state of the art
- Includes pseudonymization & encryption
- Ability to protect confidentiality, integrity, availability and resilience of processing systems and services
- Restore, Test & Report lifecycle

Concept of "security" in the NIS Act

- No commitment to the result
- No "check-list" approach
- Safeguard certain qualities / properties of an information system
- Adapted to the risks and commensurate to the state of the art
- (Identical definition in recital 49 GDPR)


Ability to resist

At a given level of confidence

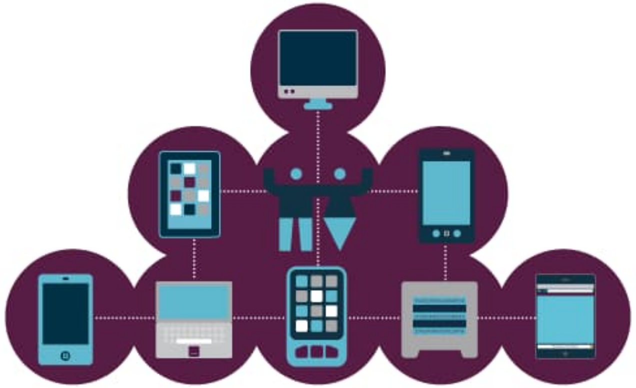
Any action that compromizes

Availability

Authenticity

Integrity

Confidentiality



Further consequences of NIS Act re: Security

General framework for IT Security in covered sectors

- Acknowledges the importance of IT systems for societal and economic activities as a whole
- Link with public order and public security

Risk-based approach to IT security

- Impact must be analysed to qualify as "incident" or "risk"
- Global preventive and organizational approach
- Still largely voluntary
- Effective enforcement powers
- Appointment of a DPO by ESO & DSS

Information sharing & cooperation

- With authorities / regulator
- Notification of incidents
- Cooperation at EU level

Complements existing rules without replacing them

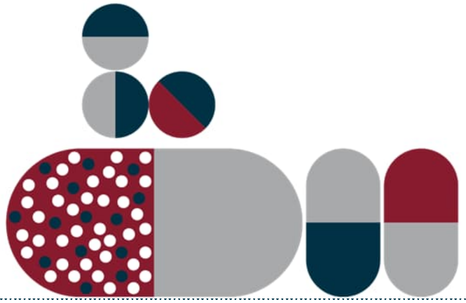
- May have an indirect impact on contractual liability

Impact of ISO 27001 under the NIS Act

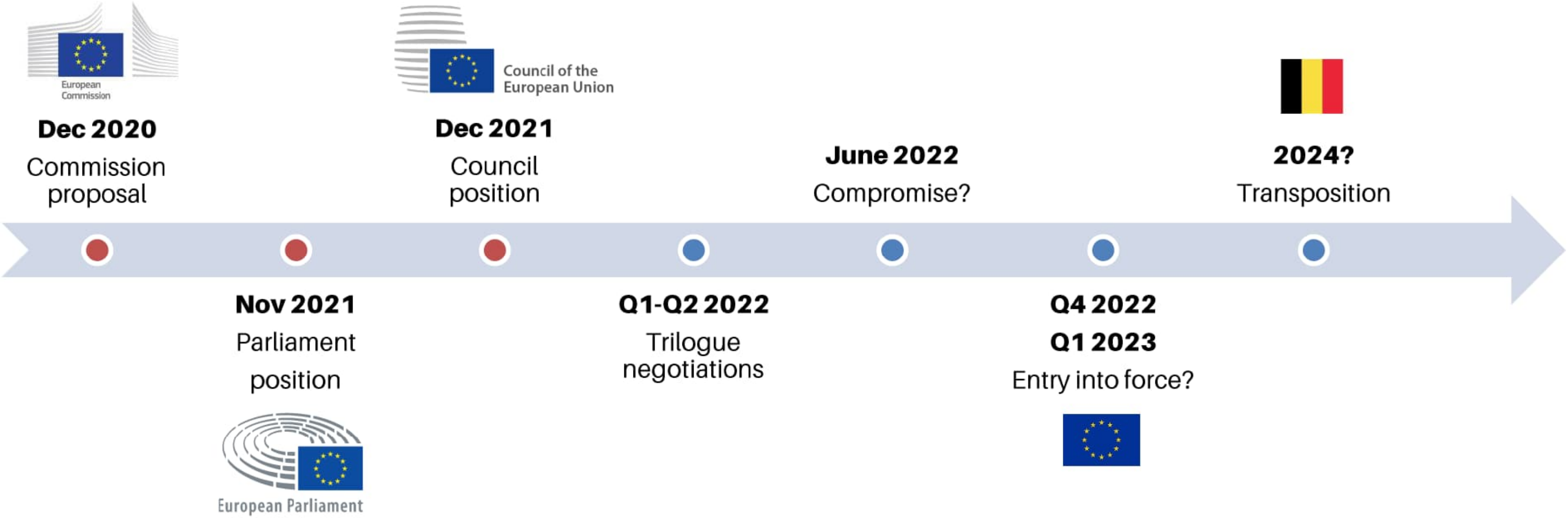
- ISO 27001 "or equivalent" norm as a clear benchmark for information security management
- Presumption of validity of IBB/PSI as verified by a competent accreditation body (rebuttable, but strong) (art. 22)
- Certification audits to replace the mandatory internal and external audits (art. 38-41)
- Clear incentive for providers to be certified… but subject to further regulatory / sectoral requirements

Certification under the Cybersecurity Act

- Regulation 2019/881 of April 17, 2019
- (ENISA mandate, rules & procedures)
- EU certification schemes for IT products, services and processes
- Voluntary basis, with EU passporting rights
- Embed security by design & by default in the manufacturing/development process, with varying levels of recognition (basic – substantial – high)



NIS2 Directive | Negotiation process



Dec 2020
Commission proposal

Nov 2021
Parliament position

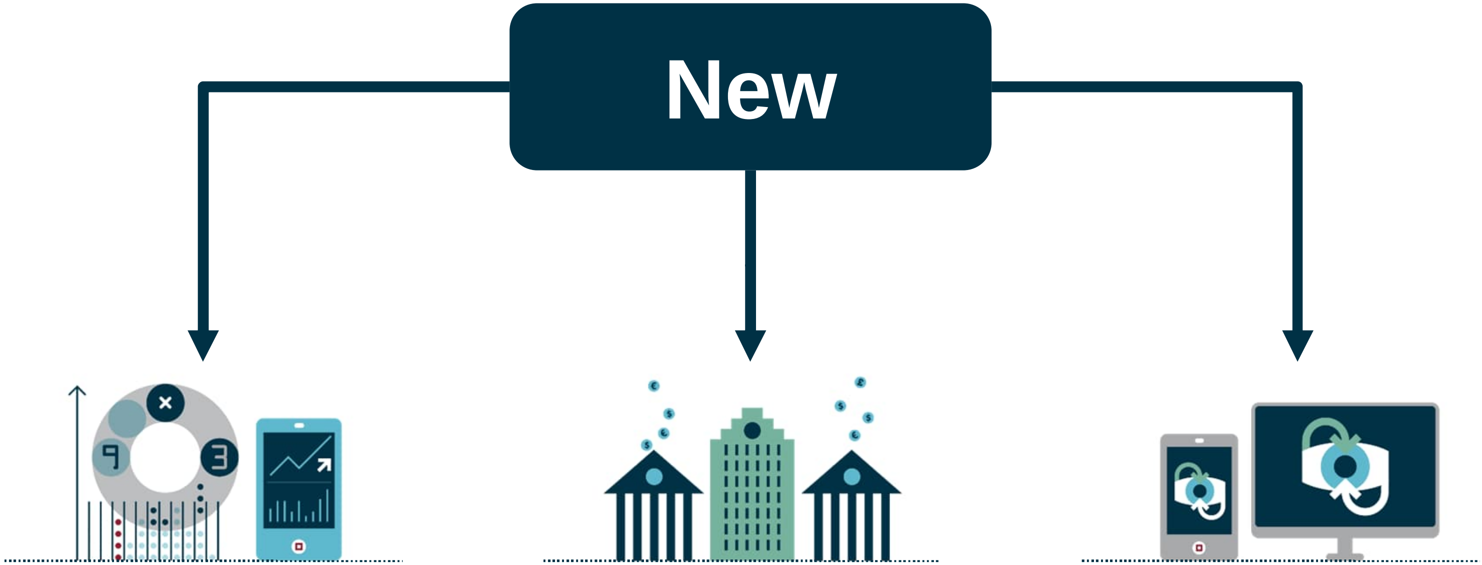
Dec 2021
Council position

Q1-Q2 2022
Trilogue negotiations

June 2022
Compromise?

Q4 2022
Q1 2023
Entry into force?

2024?
Transposition



New

New sectors

More entities

New methods of selection / identification

Entities concerned

Passive selection (instead of an active identification)

- Sectors and types of entities in the annexes
- Size: Large entities (i.e. more than 250 employees AND more than EUR 50 million annual turnover or balance sheet exceeds); and Medium entities (min 50 employees AND more than EUR 10 million turnover or balance sheet exceeds)
- Or, irrespective of size, some entities based on their essentiality or risk

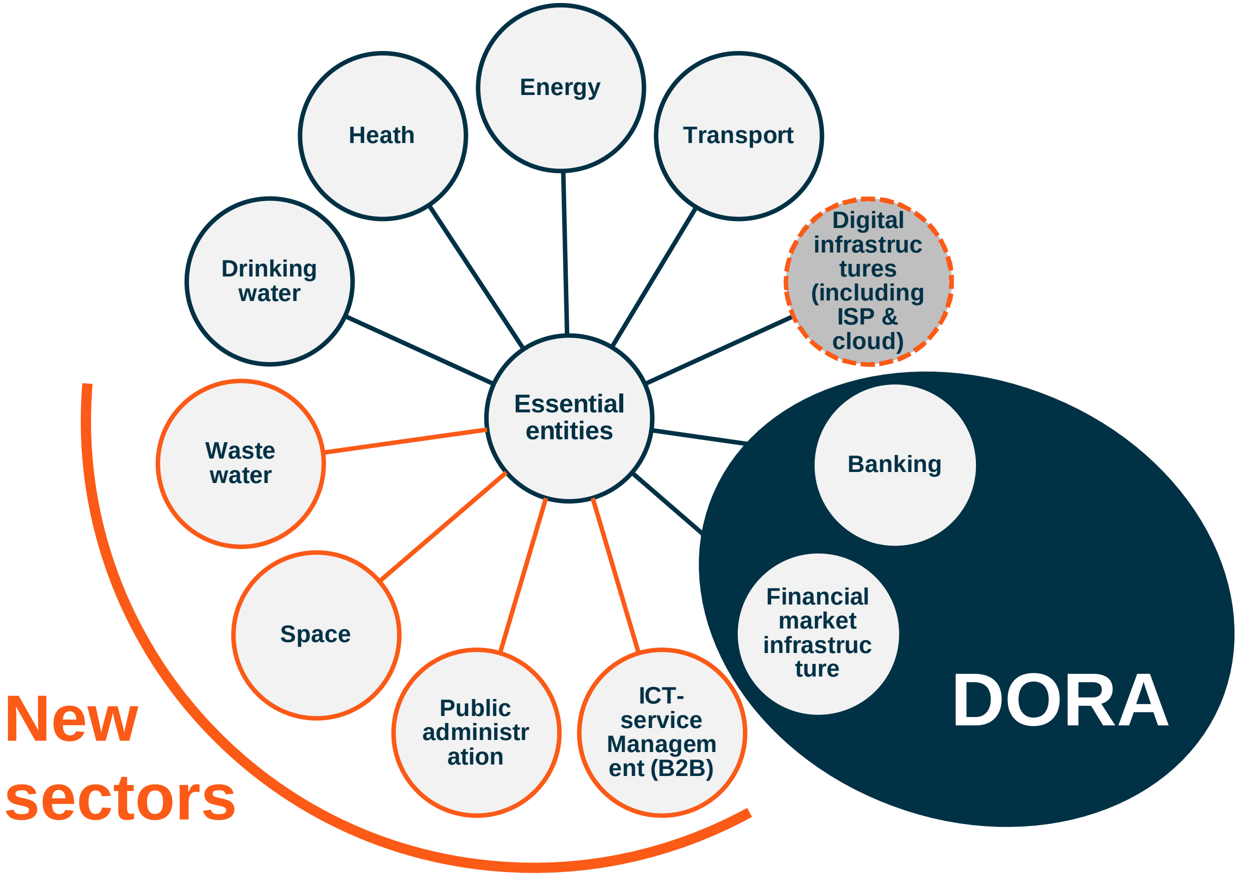
Lex generalis vs specialis: sectoral regulations at least equivalent

- e.g. DORA: finance

Essential entities vs important entities

- Essential entities: more vital sectors and especially large entities
- Important entities: medium entities, and large entities in new or less vital sectors

NIS 2 wider scope (Annex I – essential entities)



Energy

Heath

Transport

Drinking water

Digital infrastructures (including ISP & cloud)

Essential entities

Waste water

Banking

Space

Financial market infrastructure

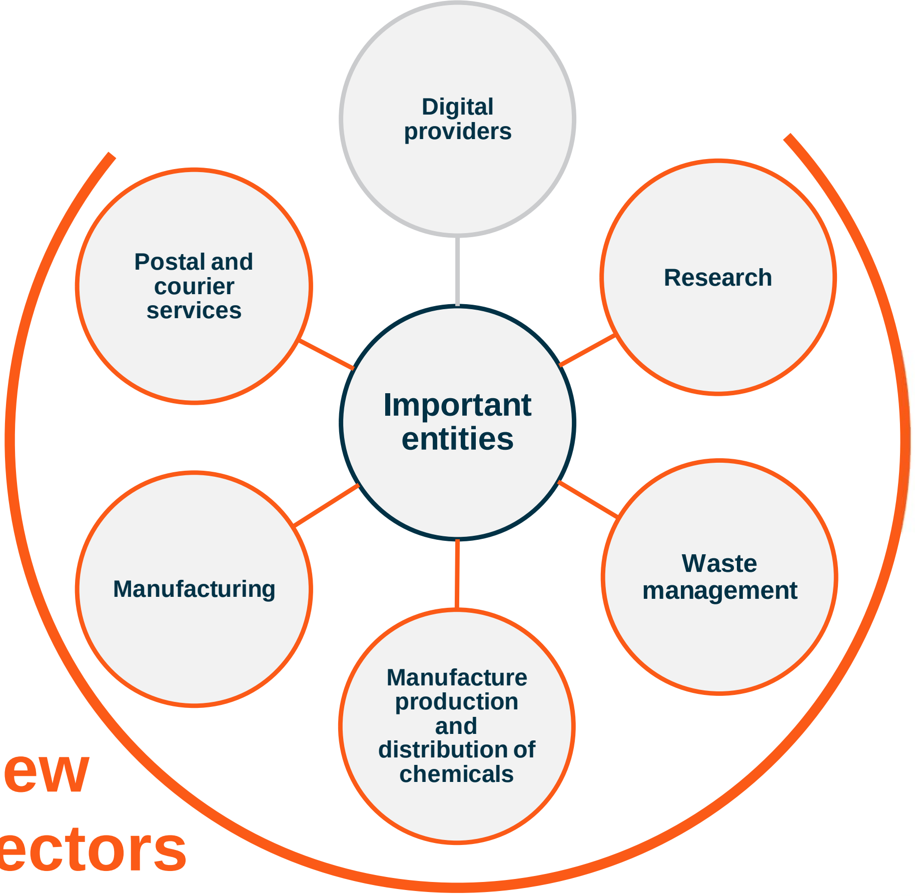
Public administration

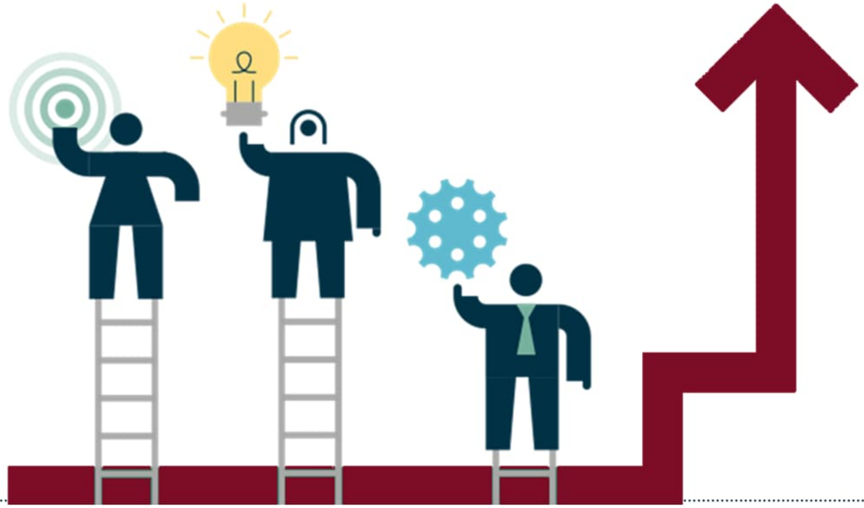
ICT-service Management (B2B)

DORA

New sectors

NIS 2 wider scope (Annex II – important entities)

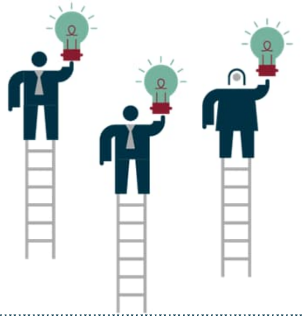




NIS 2 | Governance body

Governance Management body must :

- **approve** the cybersecurity risk management **measures**
- **oversee** cybersecurity measures **implementation**
- be liable for the non-compliance (**accountability**)
- **follow** cybersecurity **training**
- **offer** cybersecurity **training** to all employees on a regular basis



NIS 2 | Cybersecurity risk management measures

- **Appropriate** and **proportionate**
- **Manage risks posed to the security of network and information systems** which those entities use for their operations or for the provision of their services
- **Prevent or minimise the impact of incidents** on recipients of their services and on other services
- **Technical, operational and organisational measures**
- **Cost of implementation**
- **State of the art and, where applicable, relevant European and international standards**
- **Proportionality** : degree of the entity's exposure to risks, its size, the likelihood of occurrence of incidents and their severity, including their societal and economic impact

NIS 2 | Measures

All-hazards approach aiming to protect network and information systems and their physical environment from incidents, and shall include at least the following:

a) risk analysis and information system security policies

b) incident handling

c) business continuity, such as backup management and disaster recovery, and crisis management

d) supply chain security including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers

e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure

f) policies and procedures to assess the effectiveness of cybersecurity risk management measures

g) basic computer hygiene practices and cybersecurity training

h) policies and procedures regarding the use of cryptography and, where appropriate, encryption

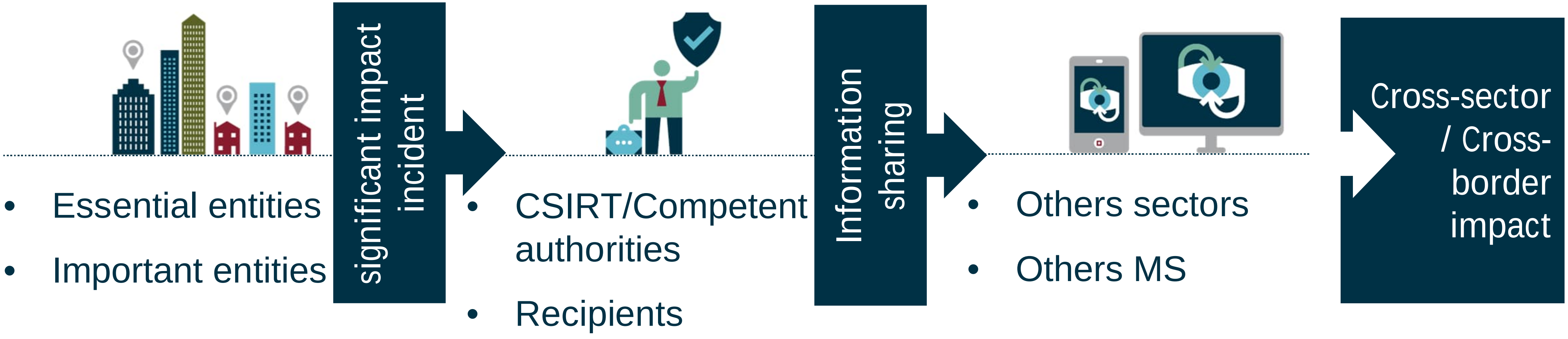
i) human resources security, access control policies and asset management

j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems within the entity, where appropriate

02 Data Breaches

Notification NIS / NIS 2

- any incident having a significant impact on the provision of their services
- without undue delay and in any event within 24 hours after having become aware of the incident (initial notification)
- CSIRT/Competent authorities
- recipients of their services (where applicable)



- Essential entities
- Important entities

significant impact incident

- CSIRT/Competent authorities
- Recipients

Information sharing

- Others sectors
- Others MS

Cross-sector / Cross-border impact

NIS 2: Significant incident

- the incident has caused or is capable of causing severe operational disruption of the service or financial losses for the entity concerned

- the incident has affected or **is capable of affecting** other natural or legal persons by causing considerable material or non-material losses.

Notification process

24h

- **Early Warning** (telephone, mail) + presumably caused by unlawful or malicious action **or could have a cross-border impact.**

72h

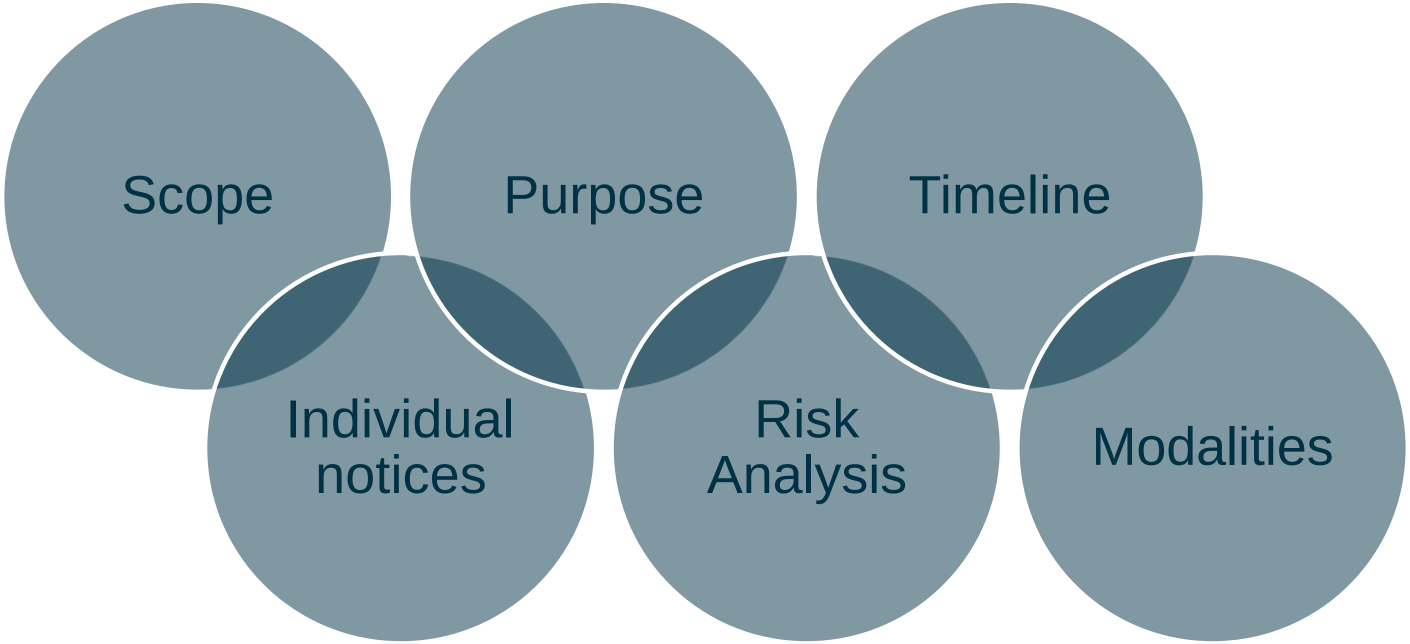
- **Initial assessment of the incident**, its severity and impact, as well as where available, the indicators of compromise.
- **Update the information.**

Update (upon request)

1 month

- **Final report** ➔ detailed description of the incident, its severity and impact.
  ➔ type of threat or root cause that likely triggered the incident.
  ➔ applied and ongoing mitigation measures.

Comparison with GDPR



Scope

Purpose

Timeline

Individual notices

Risk Analysis

Modalities

Same spirit, different modalities

Thank you

Any question?

Contact information

Benjamin Docquir

Partner

+32 2 515 9336

benjamin.docquir@osborneclarke.com

Benjamin is a Partner in Brussels and heads our Belgium IT & IP law department. An expert in intellectual property, privacy and technology law, Benjamin specialises in data security and information technology projects. He assists clients with the digital transformation of business processes and the mitigation of risks associated with information security and information management.

Interplay between NIS and GDPR in Cybersecurity

Integrated NIS & GDPR cybersecurity controls

Patrick Soenen
dpo pro secretary

22nd Nov 2022

dpo pro

INTEGRATING NIS & GDPR SECURITY

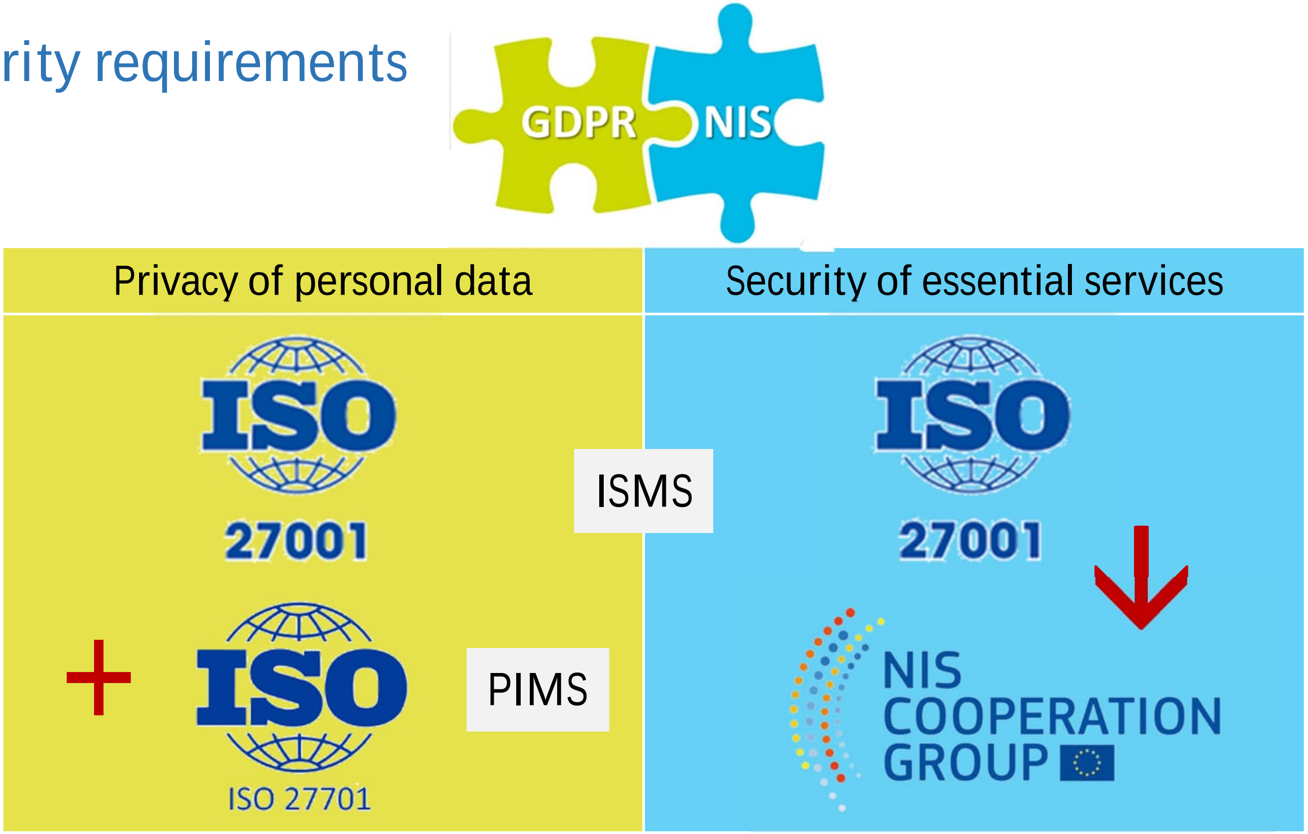
- Cyber security requirements

Art. 32 Security of processing	Art. 20 – Security Measures (Belgian NIS law)
… the controller and the processor shall implement *appropriate technical and organisational measures* to ensure a level of security appropriate to the risk…	The essential services operator shall take the necessary and *proportionate technical and organisational measures* to manage the risks to the security of the networks and information systems on which its essential services depend.
…to ensure the ongoing *confidentiality, integrity, availability*…	…the ability to resist actions that compromise the *availability, authenticity, integrity or confidentiality* of stored, transmitted or processed data and related services

No norm mentioned , but ➔ ISO 27001 explicit in Belgian NIS law

INTEGRATING NIS & GDPR SECURITY

- Cyber security requirements



Privacy of personal data

Security of essential services

ISMS

+ PIMS

No explicit ISO standard mentioned

Belgian NIS law

INTEGRATING NIS & GDPR SECURITY

NIS COOPERATION GROUP

Reference document on security measures for Operators of Essential Services

Jan 2018 .

+ Mapping

INTEGRATED NIS & GDPR SECURITY CONTROLS

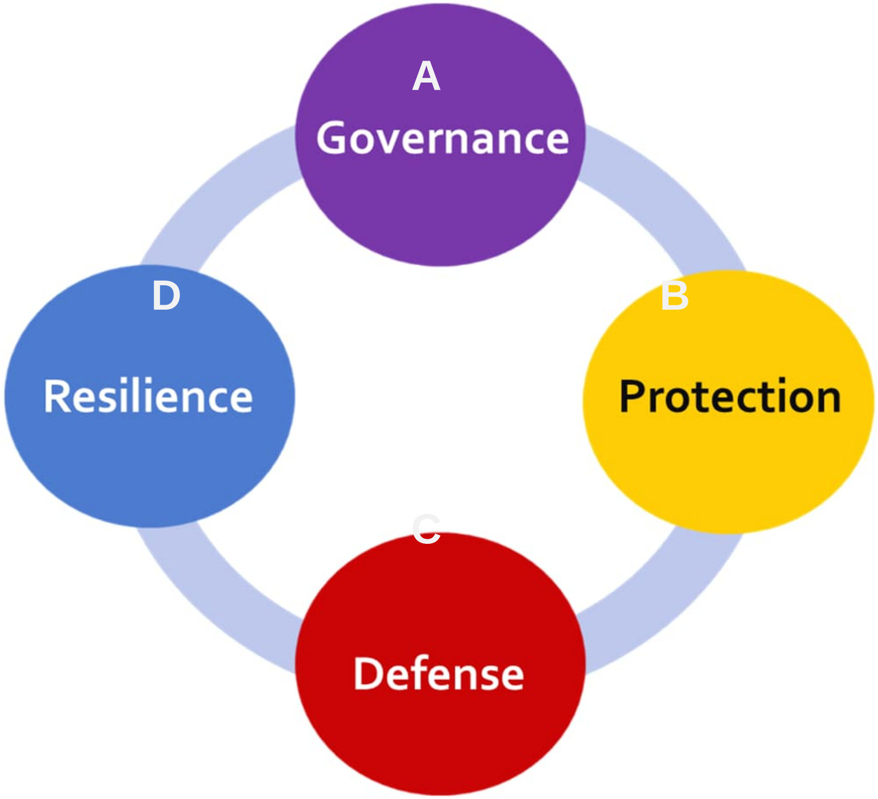
CyberSecurity Integrated FW

4 CIF domains →

11 themes

30 control objectives

75 control requirements

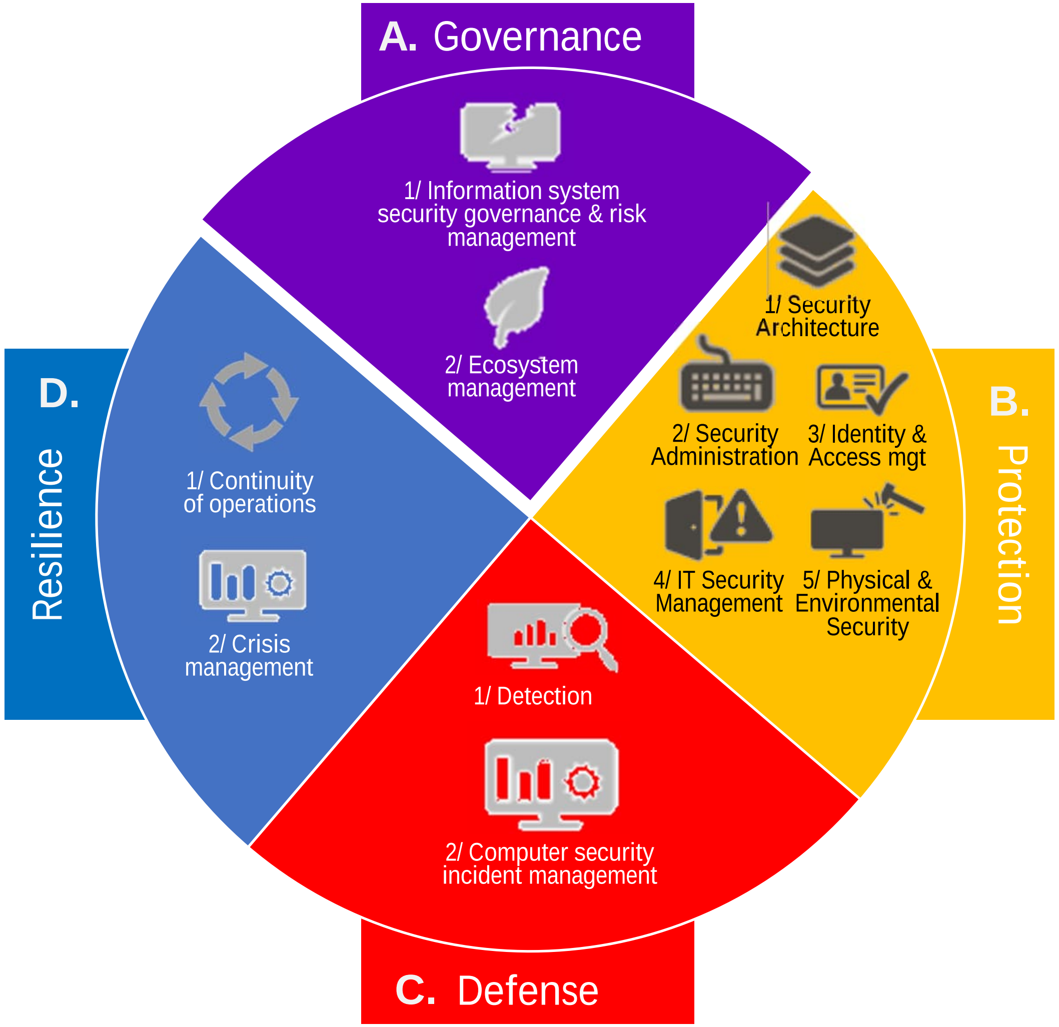


Source : ENISA

INTEGRATED NIS & GDPR SECURITY CONTROLS

CyberSecurity Integrated FW

4 CIF domains
11 themes


A. Governance
1/ Information system security governance & risk management
2/ Ecosystem management
B. Protection
1/ Security Architecture
2/ Security Administration
3/ Identity & Access mgt
4/ IT Security Management
5/ Physical & Environmental Security
C. Defense
1/ Detection
2/ Computer security incident management
D. Resilience
1/ Continuity of operations
2/ Crisis management

Source : ENISA

dpo pro

INTEGRATING NIS & GDPR SECURITY

No reference to standards, but possibly in transposed laws

See slide 19

NIS & GDPR Security Obligations: Can Common Sense Prevail?

Cybersecurity measures, at least : (NIS2 - Art. 21)	Linked to [CIF]
1. policies on risk analysis and information system security	[A.1a/b]
2. incident management	[C.2]
3. business continuity	[D.1a]
4. supply chain security (suppliers & providers)	[A.2]
5. security in systems acquisition, development & maint.	[B.4a]
6. assessment of effectiveness of cybersecurity measures	[A.1c/e]
7. cyber hygiene practices & training	[A.1f-C.1a-C.2a -D.1a/b]
8. use of cryptography, where appropriate	[B.1d]
9. hr security, access control policies & asset management	[A.1f-B.3a/b-A.1g]
10. authenticated multi-factor communication systems.	[-]

- When personal data are compromised,
  the competent authorities should cooperate and exchange information (Art. 35)

INTEGRATED NIS & GDPR SECURITY CONTROLS

CyberSecurity Integrated FW

CIF domain
2 themes
9 control objectives

A.

Governance

1/ INFORMATION SYSTEM SECURITY GOVERNANCE & RISK MGT

a. Information System Security Risk Analysis → Robust risk mgt organisation

b. Information System Security Policy → ISP & ISMS

c. Information System Security Risk Acceptance → Acceptance of residual risks

d. Information System Security Indicators → Performance evaluation

e. Information System Security Audit → Security improvements

f. Human Resource Security → Staff responsibilities

g. Asset Management → Security updates and patches

2/ ECOSYSTEM MANAGEMENT (2 control objectives)

Source : ENISA

INTEGRATED NIS & GDPR SECURITY CONTROLS

CIF domain : A. Governance

1/ INFORMATION SYSTEM SECURITY GOVERNANCE & RISK MGT

a. Info System Security Risk Analysis

A.

Governance

Control objective

The operator conducts and regularly updates a risk analysis:

NIS : identifying main risks its Critical Information Systems (CIS) underpinning the provision of the essential services (Recital 53)

GDPR : the controller or processor evaluates the risks inherent in the processing of personal data (Recital 83 - Security of Processing)

Source : ENISA/NIS/GDPR

INTEGRATED NIS & GDPR SECURITY CONTROLS

CIF domain : A. Governance

1/ INFORMATION SYSTEM SECURITY GOVERNANCE & RISK MGT

a. Info System Security Risk Analysis

A.

Governance

Control requirements	Evidence
1. Is the key personnel aware of the main information security risks and the relevant mitigations?	Personnel attendance to the training, e.g. accepted invitation, date and agenda of training, signed participation list,;;.
2. Is there a mechanism for ensuring that all security personnel use the risk management methodology and tools?	Guidance for personnel on assessing risks list of risks and evidence of updates/reviews documented
3. Is the risk management methodology and/or tools, periodically reviewed (...),	Documentation of the review process Updates of the risk mgt methodology/tools. Time-table & overall plan of the review cycle.
ISO ref. “Actions to address risks and opportunities” (27001 : 6.1 / 27701 : 5.4.1) ...	

CyberSecurity Integrated FW

CIF domain : A. Governance

1/ INFORMATION SYSTEM SECURITY GOVERNANCE & RISK MGT

a. Info System Security Risk Analysis

A.

Governance

Typical Concerns

- Lack of tone at the top for risk management
- Risk appetite not clearly established
- Lack of risk methodology / competence
- Use of different methodologies / different risk scales within business units
- Identification of IT risks instead of Enterprise risks (ERM approach needed)
- Focus on availability for NIS & confidentiality for GDPR (CIA should be covered)
- Underestimation of risk level e.g. “risk never occurred before” ….

INTEGRATED NIS & GDPR SECURITY CONTROLS

CIF domain : A. Governance

1/ INFORMATION SYSTEM SECURITY GOVERNANCE & RISK MGT

a. Info System Security Risk Analysis

A.

Governance

NIS2 (Art. 21 §2 [a])

- The measures shall be based on an all-hazards approach that aims to protect network and information systems from incidents shall include

  (a) policies on risk analysis ….

See slide 19

NIS & GDPR Security Obligations: Can Common Sense Prevail?

INTEGRATED NIS & GDPR SECURITY CONTROLS

CIF domain
5 themes
11 objectives

B.

Protection

1/ IT SECURITY ARCHITECTURE

a. Systems Configuration → Effective security measures by design

b. System Segregation → Minimised incident propagation

c. Traffic Filtering → Traffic monitoring to limit incident propagation

d. Cryptography → Protect information confidentiality & integrity

2/ IT SECURITY ADMINISTRATION

3/ IDENTITY AND ACCESS MANAGEMENT

4/ IT SECURITY MANAGEMENT

* including OT/ICS (Industrial control systems)

5/ PHYSICAL AND ENVIRONMENTAL SECURITY

Source : ENISA

INTEGRATED NIS & GDPR SECURITY CONTROLS

CyberSecurity Integrated FW

CIF domain : B. Protection

1/ IT SECURITY ARCHITECTURE

a. Systems configuration

B.

Protection

Control objective

The organisation only installs services and functionalities or connects equipment which are essential for the functioning and the security of its CIS [& personal data processing].

Additional components should be analysed according to the risk analysis.

Those components should only be used to the necessary extent and with adequate security measures. (GDPR : privacy by design & by default)

Source : ENISA

dpo pro

INTEGRATED NIS & GDPR SECURITY CONTROLS

CyberSecurity Integrated FW

CIF domain : B. Protection

1/ IT SECURITY ARCHITECTURE

a. Systems configuration

B.

Protection

Control requirements	Evidence
27. Are networks and systems supporting essential services *[& processing personal data]* configured with information security in mind?	System configuration/design policy and procedures in place and maintained. System configuration tables. Timetable and plan of system configuration /design review cycles
28. Is the effectiveness of the security configurations to protect the integrity of systems evaluated and reviewed?	Documented exercises/ tests of critical information systems in place. Timetable and plan of security configuration /design reviews.

Source : ENISA/ ISO 27k

INTEGRATED NIS & GDPR SECURITY CONTROLS

CIF domain : B. Protection

1/ IT SECURITY ARCHITECTURE

a. Systems configuration

B.

Protection

ISO 27001 control (non exhaustive)	ISO 27701
A. 4.3 Determining the scope of the information security management system	5.2.3 Include processing of personal data
A.6.2.1 Mobile device policy	6.3.2.1 Avoid compromise of personal data
A.14.1 Security requirements of information systems	6.11.1 Encrypt personal data communications over untrusted networks
A.14.2.1 Secure development policy	6.11.2.1 Policies include guidance for the processing of personal data needs
A.14.2.5 Secure system engineering principles	6.11.2.5 The principles of privacy by design and by default, and anticipate and facilitate the implementation of relevant controls on the collection and processing of personal data
A.14.2.7. Outsourced development	6.11.2.7 Application of privacy by design & by default

Source : ENISA/ ISO 27k

CyberSecurity Integrated FW

CIF domain : B. Protection
1/ IT SECURITY ARCHITECTURE
a. Systems configuration

B.

Protection

Typical Concerns

- Numerous initiatives distributed throughout the organisation
- Lack of project design methodology (security by design)
- Security design / implementation competencies
- Applicability to outsourced development
- Mobile devices not always managed (MDM)

INTEGRATED NIS & GDPR SECURITY CONTROLS

CyberSecurity Integrated FW

CIF domain
2 themes
6 objectives

C.
Defense

1/ DETECTION

a. Detection

b. Logging

c. Logs Correlation and Analysis

2/ COMPUTER SECURITY INCIDENT MANAGEMENT

a. Information System Security Incident Response → Incident handling & response process

b. Incident report → Effective & up-to-date incident reporting

c. Communication with Competent Authorities and CSIRTs → Acting on received information (NCA / CSIRTs)

Source : ENISA

INTEGRATED NIS & GDPR SECURITY CONTROLS

CyberSecurity Integrated FW

CIF domain : C. Defense

2/ COMPUTER SECURITY INCIDENT MANAGEMENT

a. Information System Security Incident Response

C.

Defense

Control objective

The operator creates and keeps up-to-date and implements a procedure for handling, response to and analysis of incidents that

- NIS :affect the functioning or the security of its CIS,
- GDPR: lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed,

in accordance with its Information System Security Policies.

Source : ENISA/ GDPR

INTEGRATED NIS & GDPR SECURITY CONTROLS

CyberSecurity Integrated FW

CIF domain : C. Defense

2/ COMPUTER SECURITY INCIDENT MANAGEMENT

a. Information System Security Incident Response

C. Defense

Control requirements	Evidence
59. Is there a policy, along with related processes or systems, in place for incident response?	Documented incident analysis policy, addressing purpose, scope, roles and responsibilities and coordination among all related entities.
60. Is there a mechanism to ensure that the incident response staff is available and properly trained to manage and handle incidents?	Records of incident response related training sessions to the appropriate personnel.
61. Is the incident response policy and procedures reviewed following an incident?	Policies and review of tools and procedures for Incident detection and analysis
62. Are there any incident handling processes in place in accordance with industry standards and good practices?	Management commitment with the incident response policy, guidelines and procedures.

Source : ENISA

INTEGRATED NIS & GDPR SECURITY CONTROLS

CyberSecurity Integrated FW

CIF domain : C. Defense
2/ COMPUTER SECURITY INCIDENT MANAGEMENT
a. Information System Security Incident Response

C.

Defense

Typical Concerns

- Non-integrated incident management processes
  i.e., specific NIS procedure by CISO / specific GDPR procedure by DPO
- Lack of staff awareness / competencies
- Slow response process / unaligned with incident criticality

INTEGRATED NIS & GDPR SECURITY CONTROLS

CIF domain : C. Defense
2/ COMPUTER SECURITY INCIDENT MANAGEMENT
a. Information System Security Incident Response

C.

Defense

NIS2

- (Recital 86) …
  - managed security service providers play an important role in assisting entities in their efforts
  - to prevent, detect, respond to or recover from incidents
  - in areas such as incident response, penetration testing, security audits and consultancy.

INTEGRATED NIS & GDPR SECURITY CONTROLS

CyberSecurity
Integrated
FW

CIF domain
2 themes
4 objectives

D.
Resilience

1/ CONTINUITY OF OPERATIONS

a. Business Continuity Mgt → Effective security measures

b. Disaster Recovery Procedures → Deployed DRP capabilities

2/ CRISIS MANAGEMENT

a. Crisis mgt organisation → Roles & Responsibilities

b. Crisis mgt process → Formal documented procedure

CIF domain : D. Resilience

1/ CONTINUITY OF OPERATIONS

a. Business Continuity Management

D.

Resilience

Control objective

The organisation defines objectives and strategic guidelines regarding business continuity management, in case of IT (major) security incident.

Guidance applicable for NIS and GDPR

Source : ENISA

INTEGRATED NIS & GDPR SECURITY CONTROLS

CIF domain : D. Resilience

1/ CONTINUITY OF OPERATIONS

a. Business Continuity Management

D.

Resilience

Control requirements	Evidence
68. Has a business continuity strategy for the critical services provided by the organisation been implemented?	Formally documented service continuity strategy, including recovery time objectives for key services and processes.
69. Are contingency plans for the systems supporting essential services (NIS) and personal data processing (GDPR) implemented in the organisation?	Contingency plans for critical systems, including procedures for common threats, triggers for activation, steps and recovery time objectives.
70. Are all personnel involved in the continuity operations properly trained in their roles and responsibilities with regards to the information system?	Records of individual training activities as well as post-exercise reports.

Source : ENISA/ GDPR

CyberSecurity Integrated FW

CIF domain : D. Resilience

1/ CONTINUITY OF OPERATIONS

a. Business Continuity Management

D.

Resilience

Typical Concerns

- Incomplete / inadequate Business Impact Analysis
- Lack of contingency plans
- DRP procedures without related BCP
- Outdated BPC/DRP procedures
- Absence of BCP/DRP testing
- Lack of staff readiness

CyberSecurity Integrated FW

CIF domain : D. Resilience

1/ CONTINUITY OF OPERATIONS

a. Business Continuity Management

D.

Resilience

NIS2

(Art 21) ... Cybersecurity measures, at least :

(c) business continuity, such as backup management and disaster recovery, and crisis management

SUMMARY

Based on

NIS COOPERATION GROUP

ISO 27001

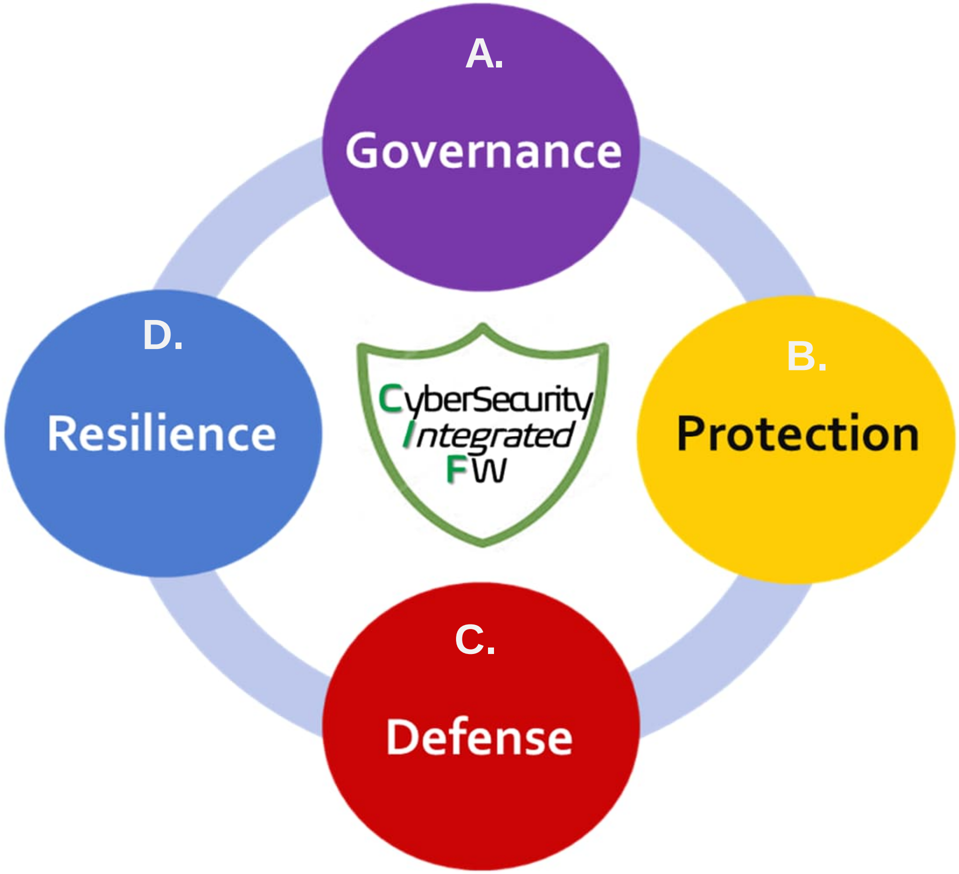
ISO 27701

4 CIF domains

11 themes

30 control objectives

75 control requirements



CRITICAL SUCCESS FACTORS

CyberSecurity
Integrated
FW

- Management support
- Enterprise wide approach
- Competent and adequate resources
- Cooperation between stakeholders namely CISO, DPO, business, IT, ….
- Implementation of internal control (monitoring)

dpo pro

INFORMATION SOURCES

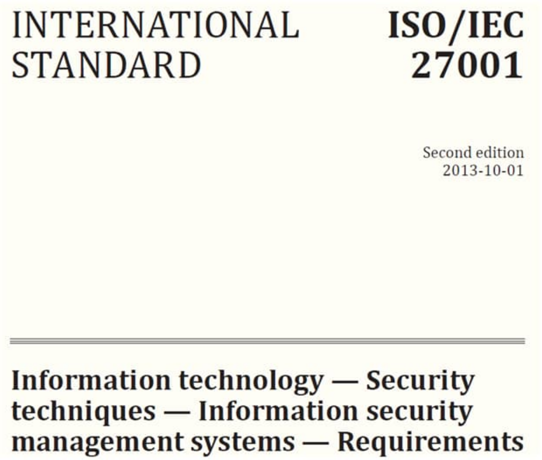
Reference document on security measures for Operators of Essential Services

CG Publication 01/2018

enisa

AUDIT REPORT
RISK ASSESSMENT

Guidelines on assessing DSP and OES compliance to the NISD security requirements



INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

INTERNATIONAL STANDARD

ISO/IEC 27701

First edition
2019-08

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

dpo pro

join us on in
www.dpopro.be
www.dpoconnect.be

Benefits from joining dpo pro

- Networking
- dpo pro Mag
- Documents sharing
- Workgroups
- dpo connect
- Conferences and Webinars
- Partners benefits
- Access to GDPR-Tools
- And your representation in our Professional Union

Our partners

Data Protection institute

ISACA Belgium Chapter

CYBER SECURITY COALITION.be

THANK
YOU!

Q
A

Interplay between NIS and GDPR in Cybersecurity

Compliance & Security in a Microsoft Ecosystem

Stephan Van Dyck

November 22, 2022

ISACA®
Belgium Chapter

About myself

- Freelance Security Architect
- Microsoft Certified Trainer
- Several Security Certifications
- Hobby turned into profession

ISACA
Belgium Chapter

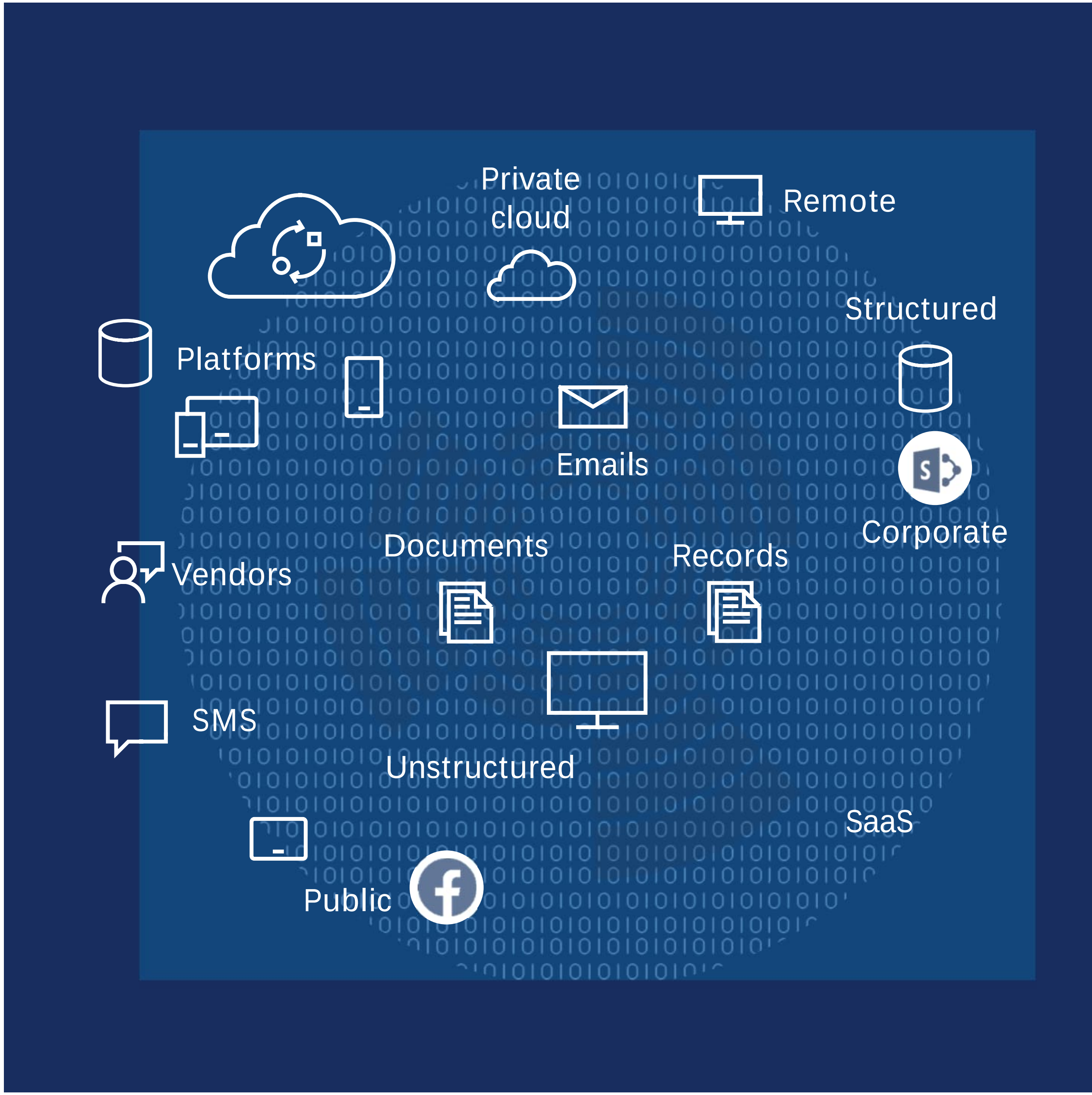
Agenda

- The data explosion challenge
- Structured vs unstructured data
- Data visibility
- Demo based on a true usecase

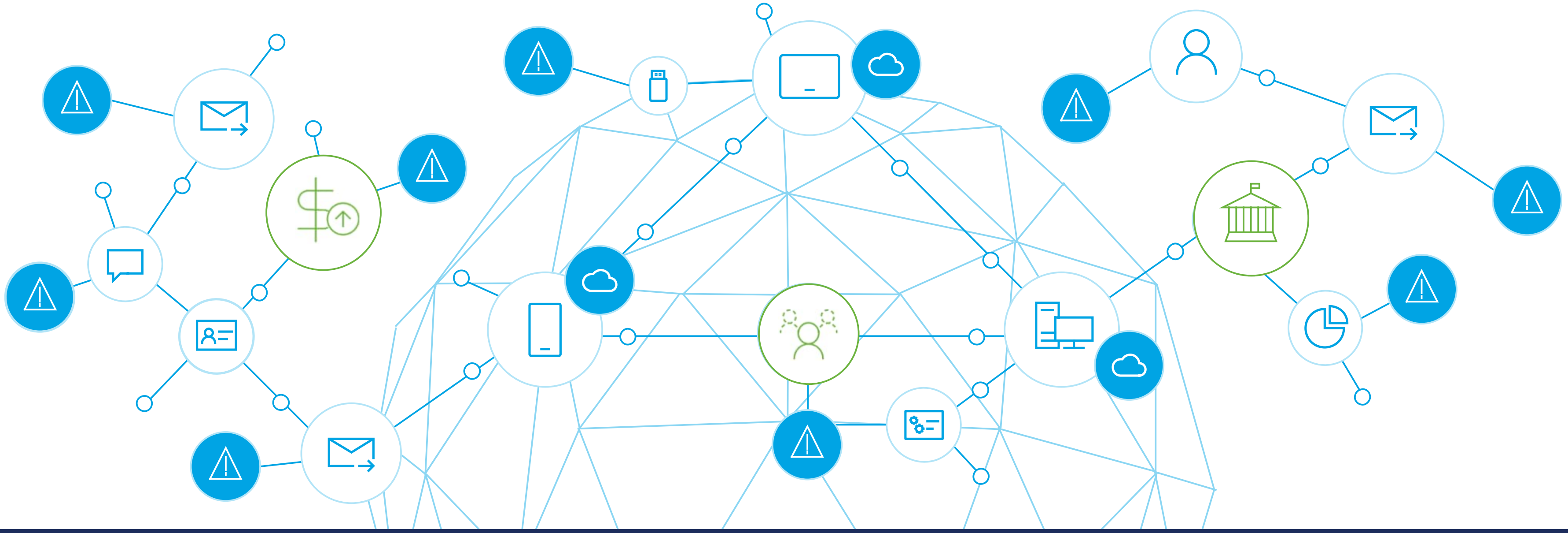
ISACA Belgium Chapter

Data is exploding

It’s created, stored, and shared everywhere



Compliance and privacy realities



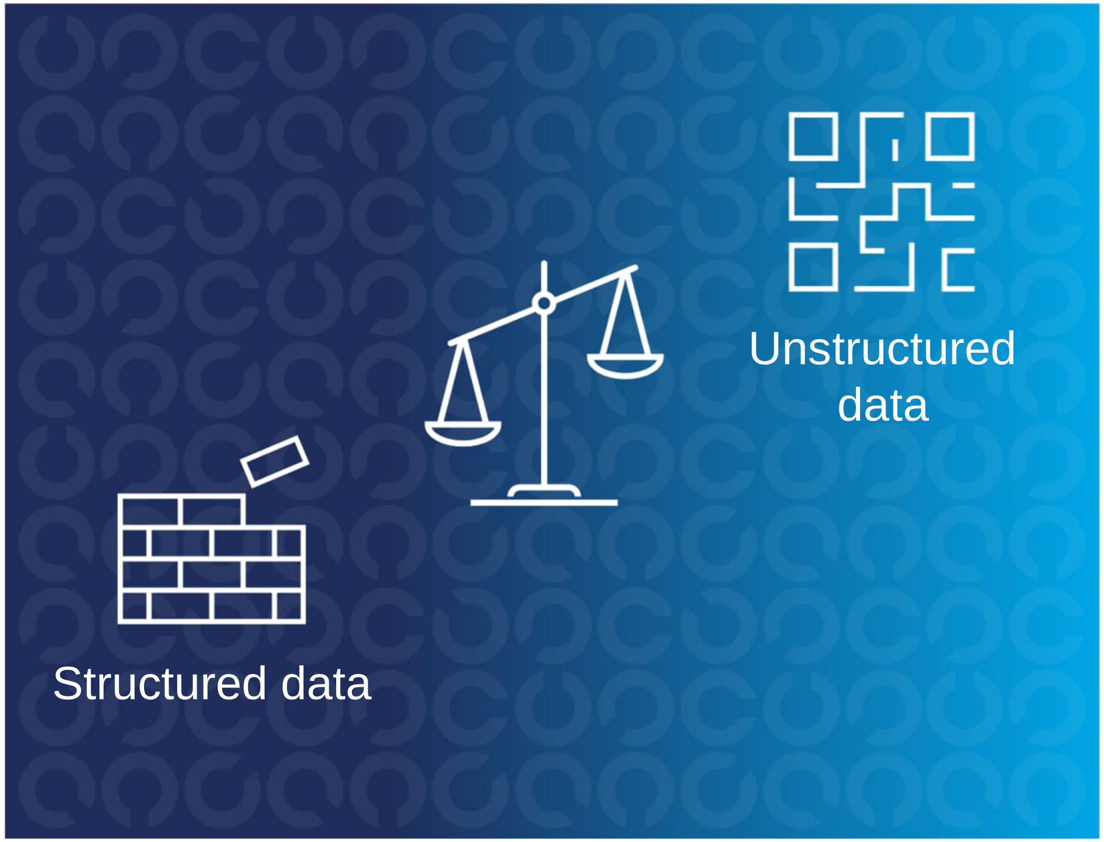
We need to manage the continuous data explosion and increasing costs

We are limited with available staff and resources to manage the scale necessary

We need to be prepared for increased accountability due to complexity of regulatory

Structured vs unstructured data

- Imbalance between controls on structured vs unstructured data
- Organization driven vs User driven
- Data residency
- Limited visibility on unstructered data

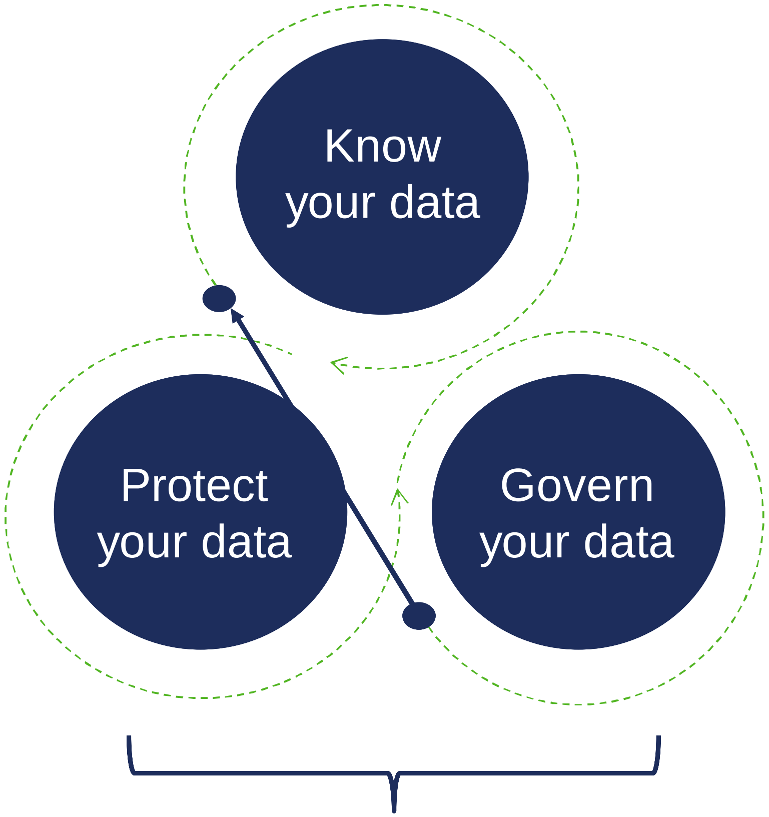


ISACA
Belgium Chapter

Information Protection & Governance

Protect and govern data, wherever it can be found

Understand your data landscape and identify important data



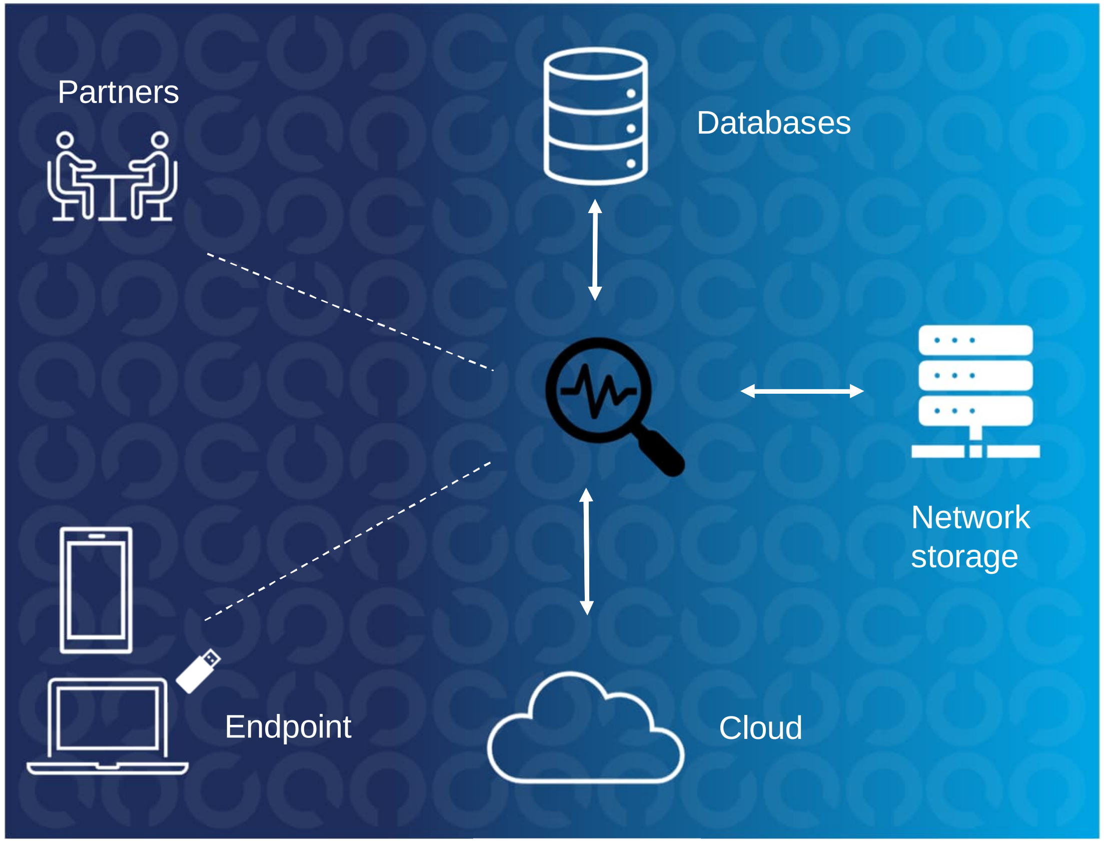
Apply flexible protection actions including encryption, access controls and visual markings

Automatically retain, delete and store data records in a compliant manner

Microsoft Purview
Unified data governance platform

What is outsite your line of sight?

- What could leave the building is generally speaking our of control
- Tools have gaps when it comes to protecting data where it matters
- You can’t protect what you can’t see
- Policy without enforcement is just a suggestion



ISACA
Belgium Chapter

Demo

Data protection for a health care provider

ISACA® Belgium Chapter

Case study

- Healthcare provider in Belgium
- Doctors using O365 tools on mobile devices
- Data should only be stored in sactioned sources

Usecase:

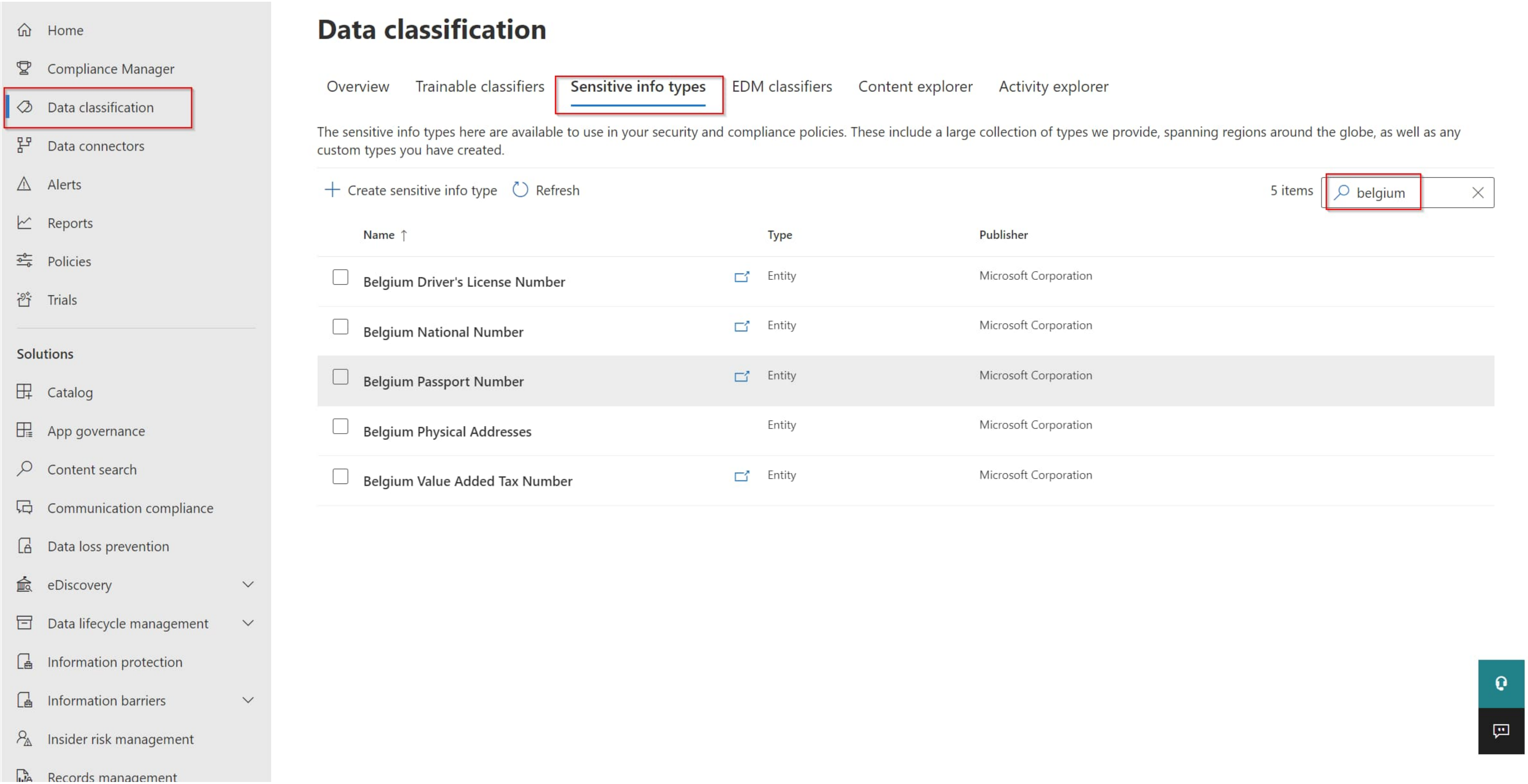
- Detect sensitive data in unsactioned data stores
- Unique identifier: RIZIV number
- Detect gaps in the security / data protection policy
- How to enforce the policy

Check list

- On-prem network drives
- Sharepoint on-prem and Online
- O365 and Azure
- iOS, Android and Windows 10
- Focus on unstructured data

- Patient info should be stored on-prem and can only be shared with limited number of people

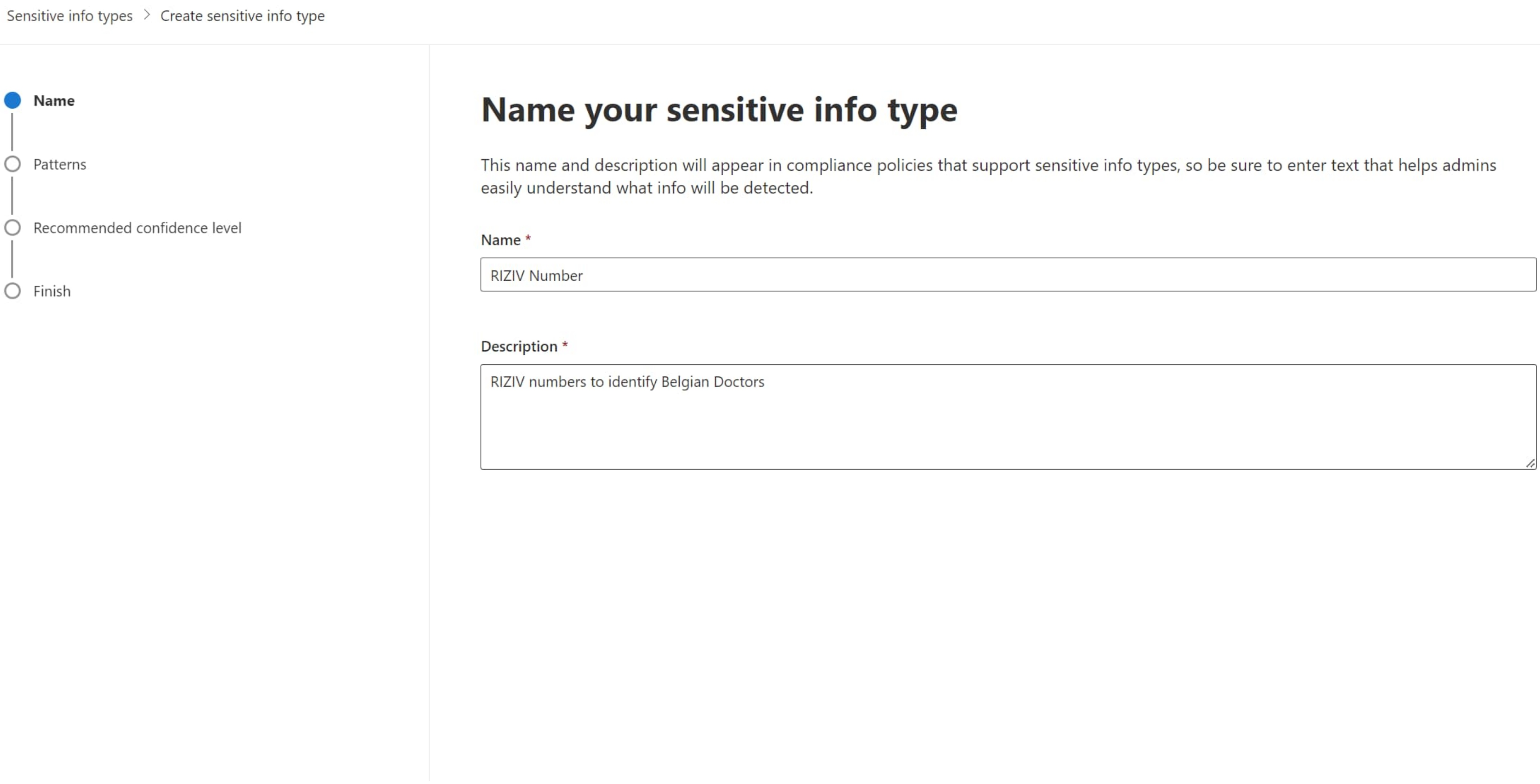
Purview portal: Sensitive info types



Data classification

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

	Name ↑	Type	Publisher
□	Belgium Driver's License Number	Entity	Microsoft Corporation
□	Belgium National Number	Entity	Microsoft Corporation
□	Belgium Passport Number	Entity	Microsoft Corporation
□	Belgium Physical Addresses	Entity	Microsoft Corporation
□	Belgium Value Added Tax Number	Entity	Microsoft Corporation


Sensitive info types > Create sensitive info type
● Name
○ Patterns
○ Recommended confidence level
○ Finish

Name your sensitive info type

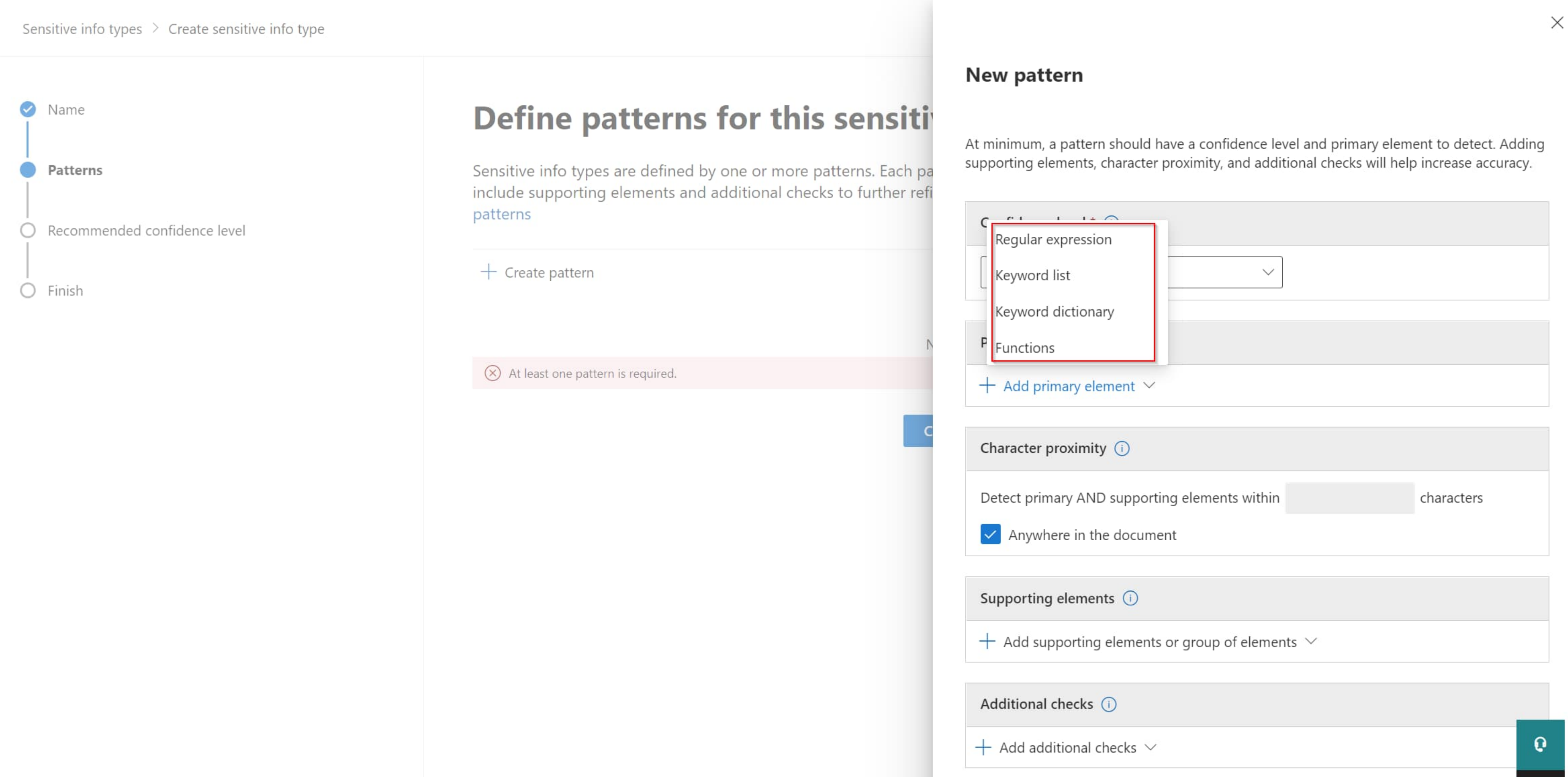
This name and description will appear in compliance policies that support sensitive info types, so be sure to enter text that helps admins easily understand what info will be detected.

Name *

RIZIV Number

Description *

RIZIV numbers to identify Belgian Doctors



Sensitive info types > Create sensitive info type

Define patterns for this sensiti

Sensitive info types are defined by one or more patterns. Each pa include supporting elements and additional checks to further refi patterns

ⓧ At least one pattern is required.

New pattern

At minimum, a pattern should have a confidence level and primary element to detect. Adding supporting elements, character proximity, and additional checks will help increase accuracy.

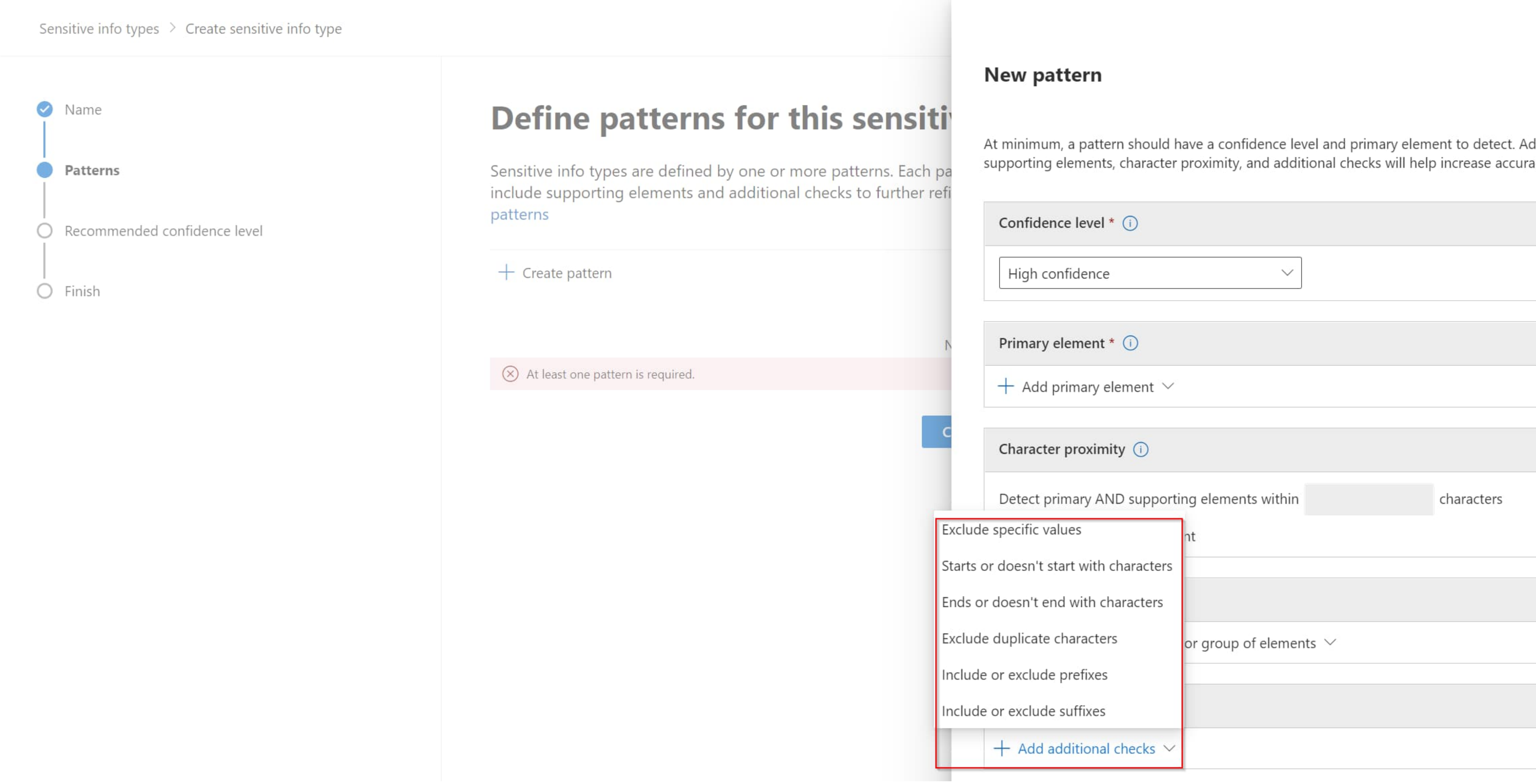
Character proximity ⓘ

Detect primary AND supporting elements within characters

☑ Anywhere in the document

Supporting elements ⓘ

Additional checks ⓘ



Sensitive info types > Create sensitive info type

- Name
- Patterns
- Recommended confidence level
- Finish

Define patterns for this sensiti

Sensitive info types are defined by one or more patterns. Each pa include supporting elements and additional checks to further refi patterns

+ Create pattern

N

At least one pattern is required.

C

New pattern

At minimum, a pattern should have a confidence level and primary element to detect. Ad supporting elements, character proximity, and additional checks will help increase accura

Confidence level *

High confidence

Primary element *

+ Add primary element

Character proximity

Detect primary AND supporting elements within characters

nt

or group of elements

Exclude specific values

Starts or doesn't start with characters

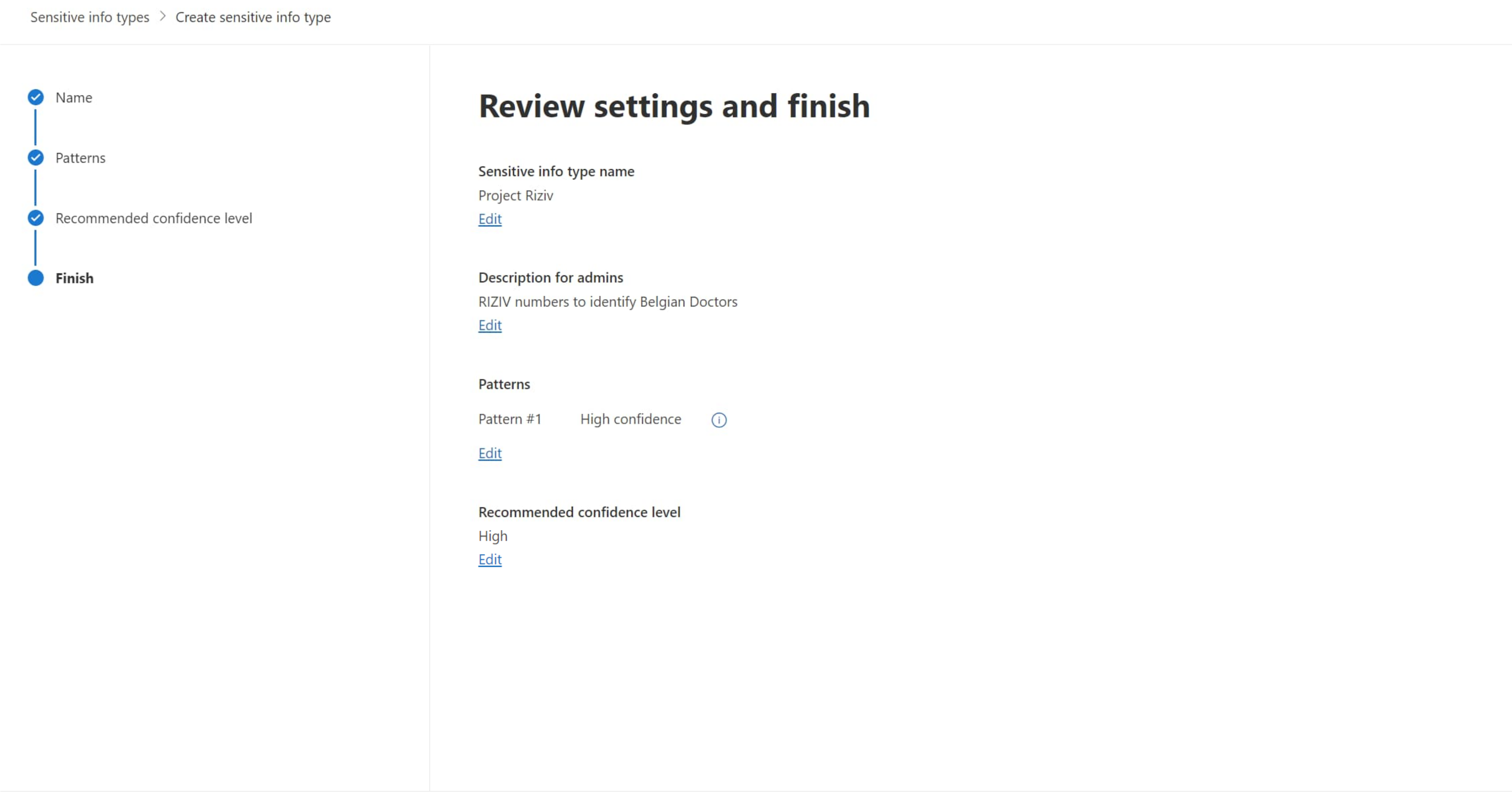
Ends or doesn't end with characters

Exclude duplicate characters

Include or exclude prefixes

Include or exclude suffixes

+ Add additional checks



Sensitive info types > Create sensitive info type

✓ Name

✓ Patterns

✓ Recommended confidence level

● **Finish**

Review settings and finish

Sensitive info type name

Project Riziv

Edit

Description for admins

RIZIV numbers to identify Belgian Doctors

Edit

Patterns

Pattern #1 High confidence ⓘ

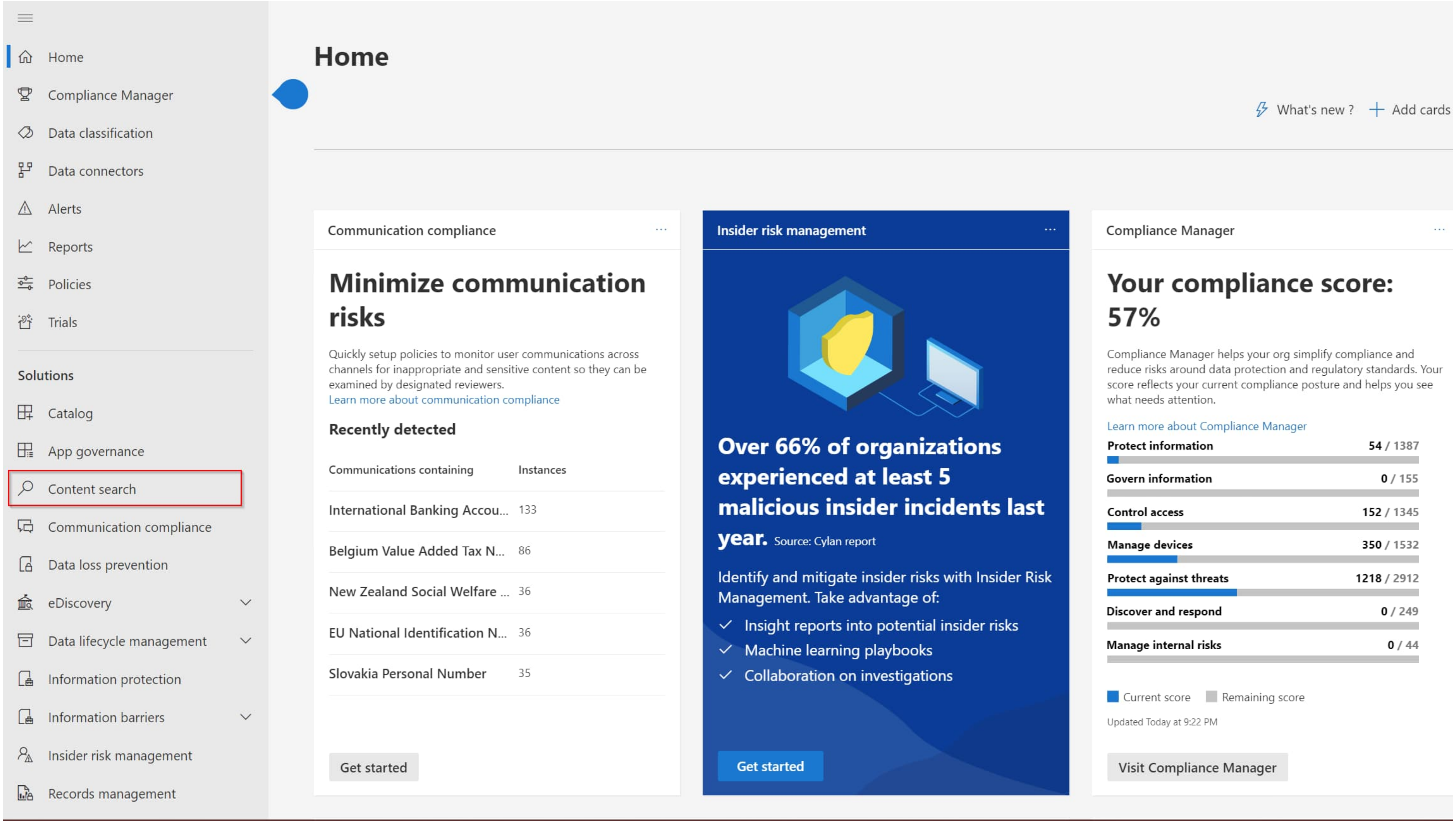
Edit

Recommended confidence level

High

Edit

Content Search



Home

Communication compliance

Minimize communication risks

Quickly setup policies to monitor user communications across channels for inappropriate and sensitive content so they can be examined by designated reviewers.
Learn more about communication compliance

Recently detected

Communications containing	Instances
International Banking Accou...	133
Belgium Value Added Tax N...	86
New Zealand Social Welfare ...	36
EU National Identification N...	36
Slovakia Personal Number	35

Insider risk management

Over 66% of organizations experienced at least 5 malicious insider incidents last year. Source: Cylan report

Identify and mitigate insider risks with Insider Risk Management. Take advantage of:

- ✓ Insight reports into potential insider risks
- ✓ Machine learning playbooks
- ✓ Collaboration on investigations

Compliance Manager

Your compliance score: 57%

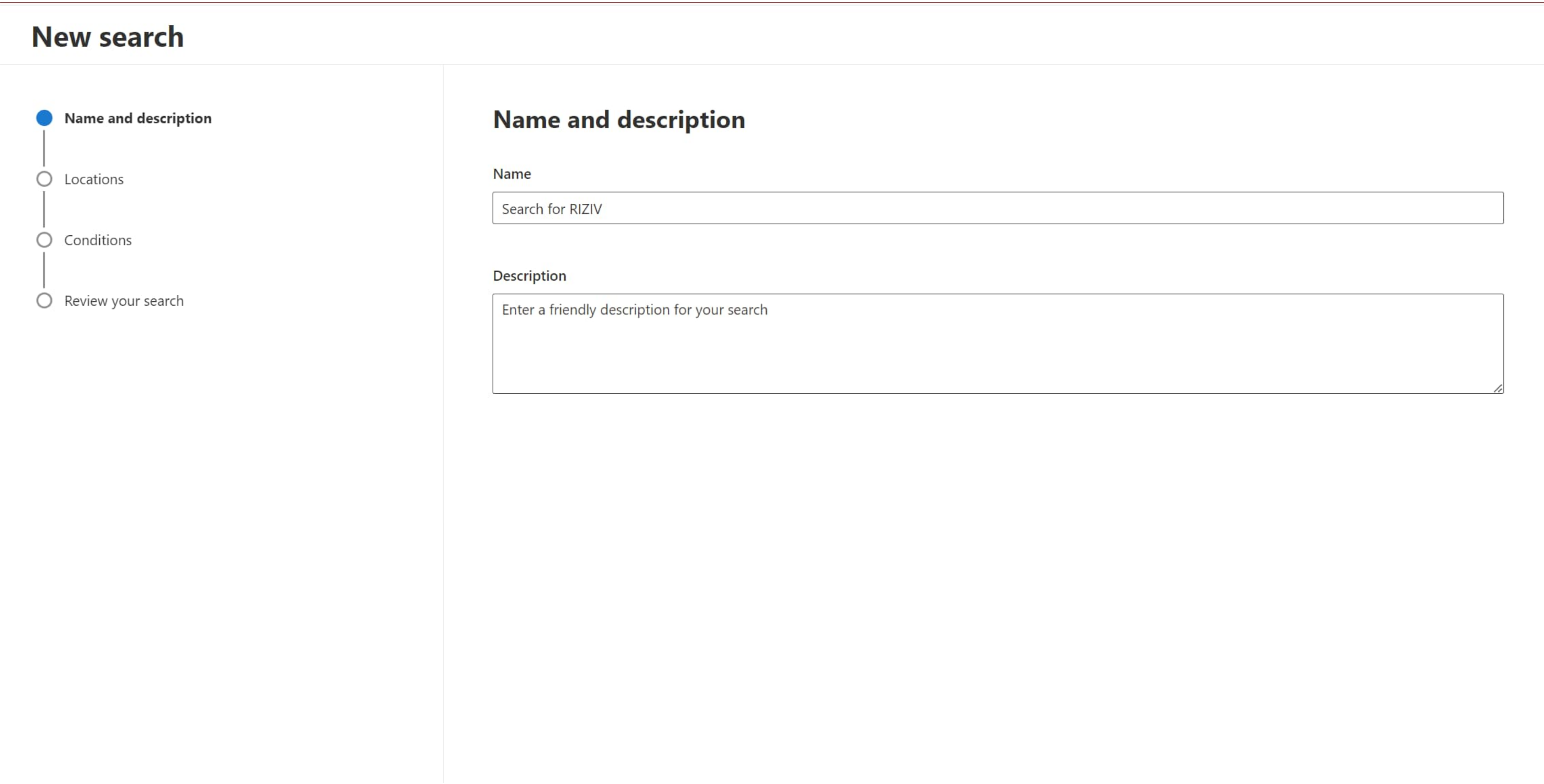
Compliance Manager helps your org simplify compliance and reduce risks around data protection and regulatory standards. Your score reflects your current compliance posture and helps you see what needs attention.

Learn more about Compliance Manager

Protect information	54 / 1387
Govern information	0 / 155
Control access	152 / 1345
Manage devices	350 / 1532
Protect against threats	1218 / 2912
Discover and respond	0 / 249
Manage internal risks	0 / 44

🟦 Current score ▨ Remaining score

Updated Today at 9:22 PM



New search

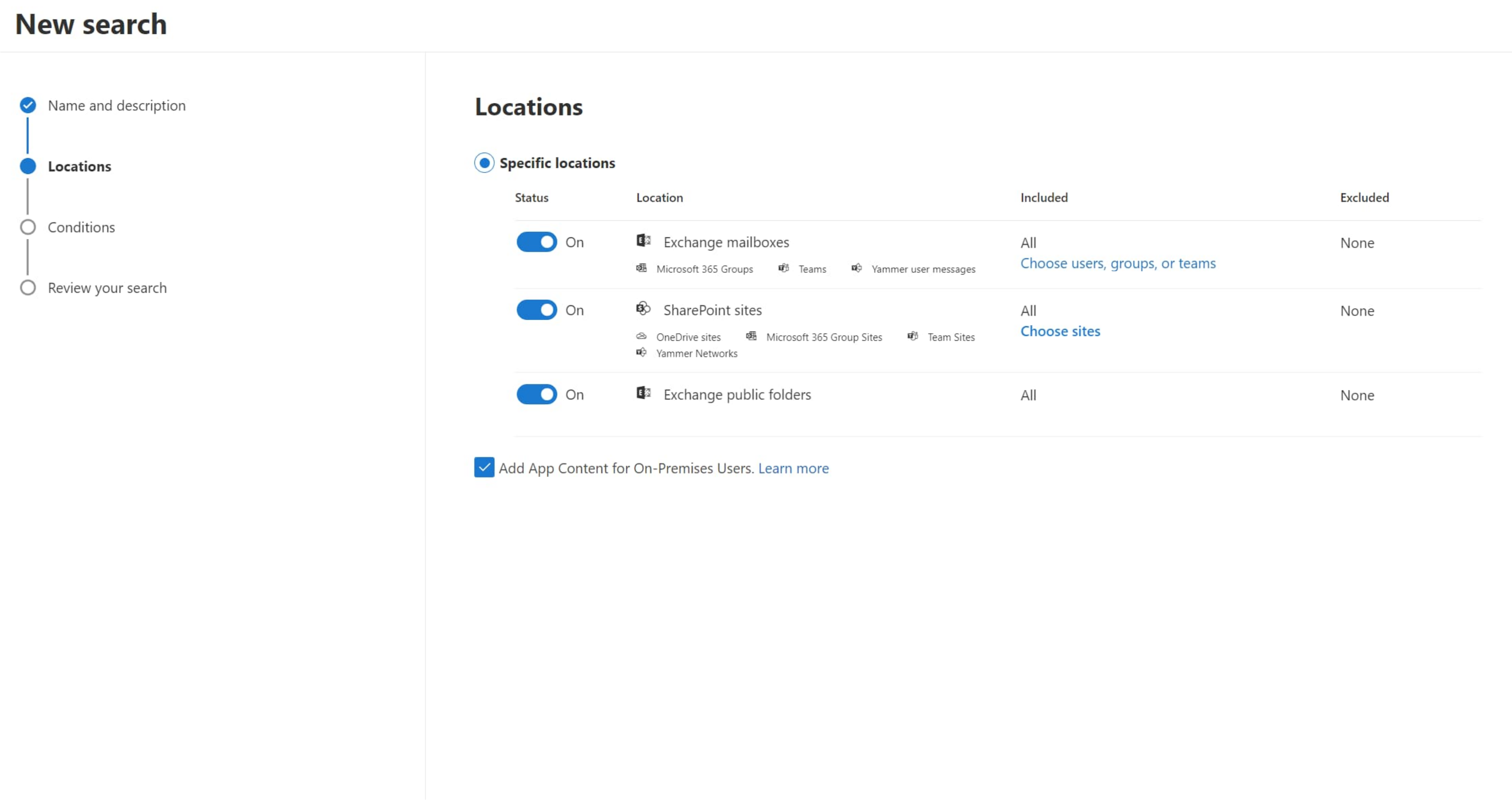
Name and description

Name

Search for RIZIV

Description

Enter a friendly description for your search



New search

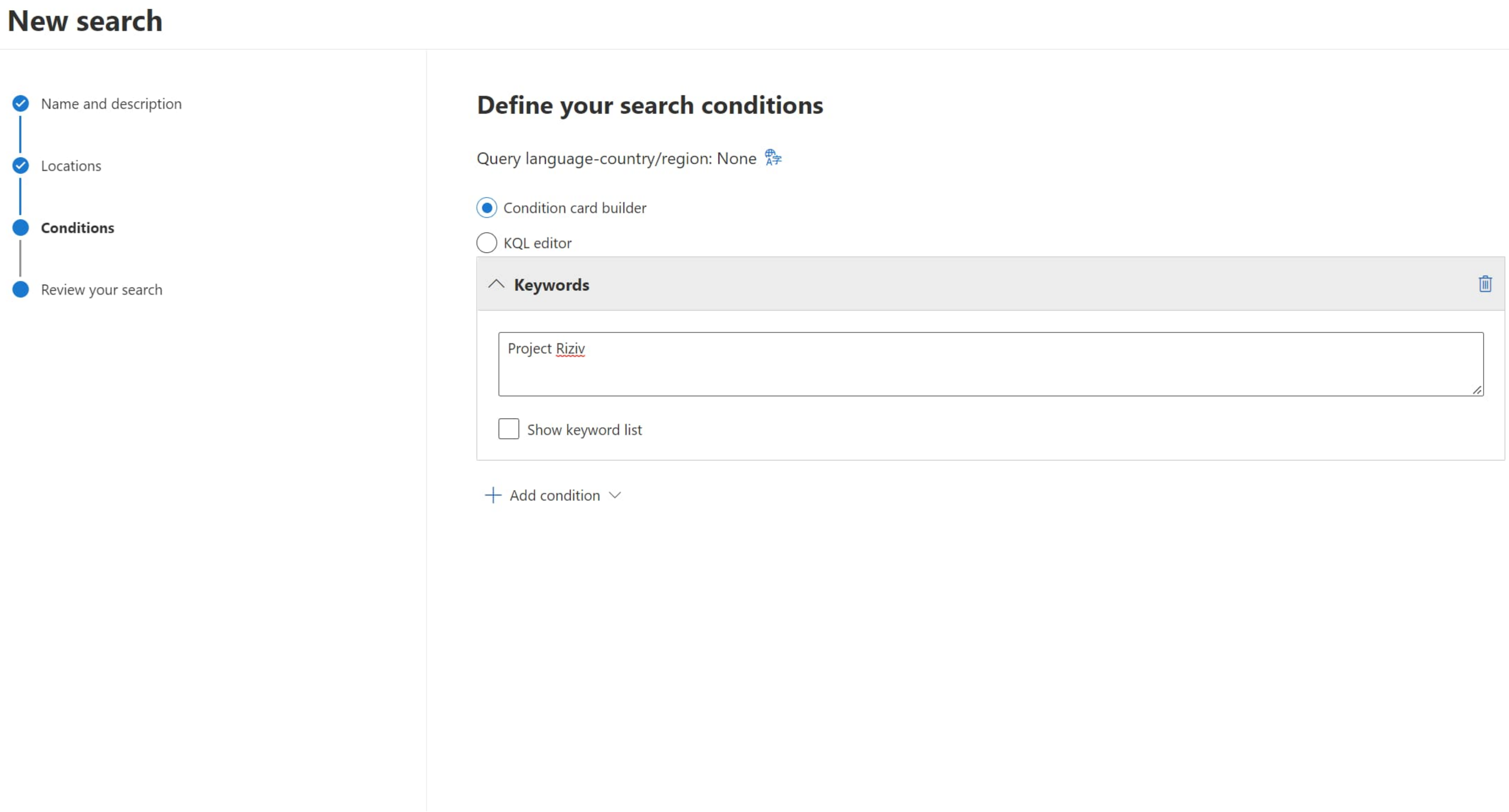
- ✓ Name and description
- ● **Locations**
- ○ Conditions
- ○ Review your search

Locations

● **Specific locations**

Status	Location	Included	Excluded
On	Exchange mailboxes Microsoft 365 Groups Teams Yammer user messages	All Choose users, groups, or teams	None
On	SharePoint sites OneDrive sites Microsoft 365 Group Sites Team Sites Yammer Networks	All Choose sites	None
On	Exchange public folders	All	None

☑ Add App Content for On-Premises Users. Learn more



New search

- ✓ Name and description
- ✓ Locations
- ● **Conditions**
- ● Review your search

Define your search conditions

Query language-country/region: None

● Condition card builder

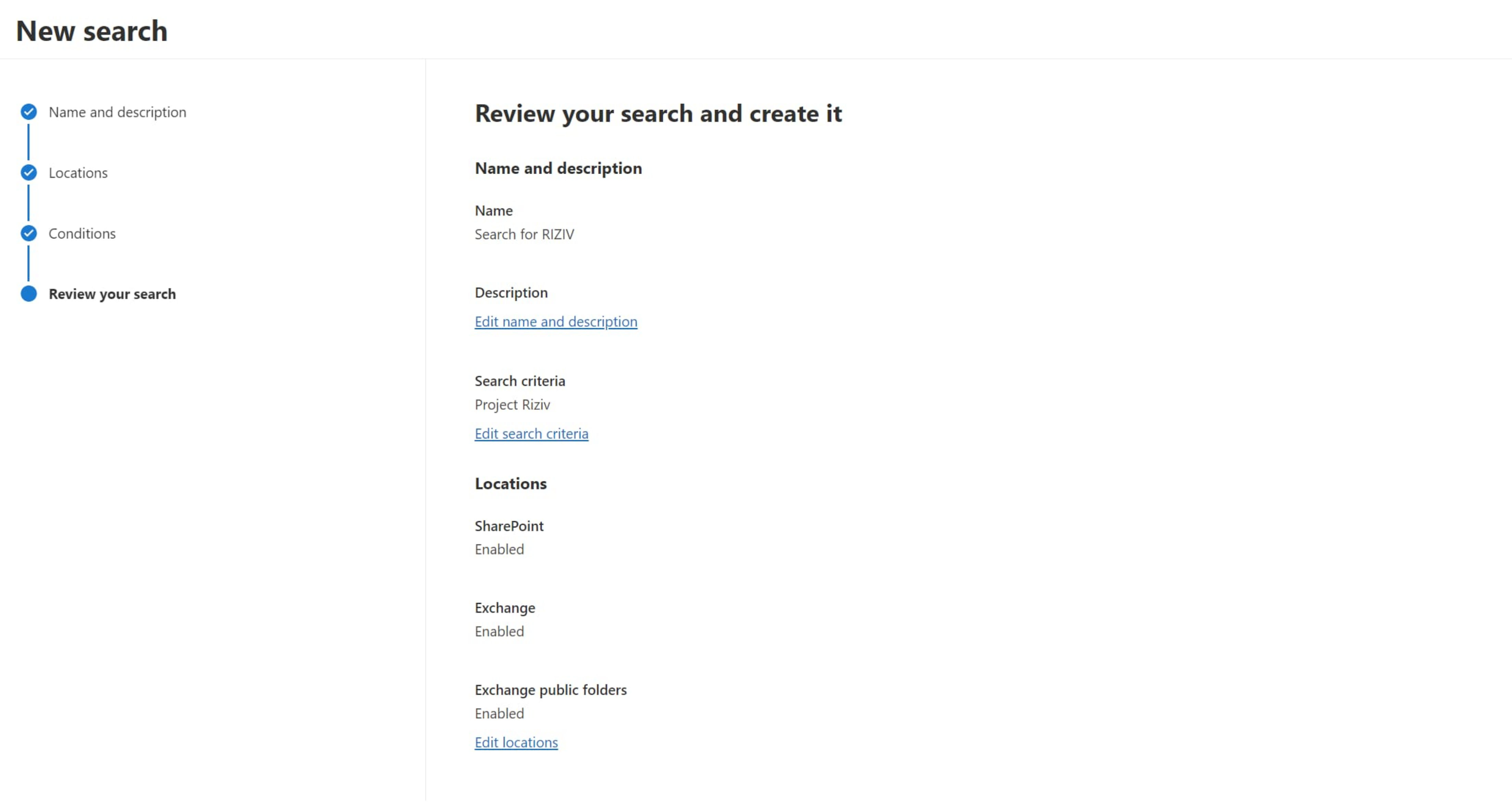
○ KQL editor

Keywords

Project Riziv

□ Show keyword list

+ Add condition



New search

✓ Name and description

✓ Locations

✓ Conditions

● **Review your search**

Review your search and create it

Name and description

Name

Search for RIZIV

Description

Edit name and description

Search criteria

Project Riziv

Edit search criteria

Locations

SharePoint

Enabled

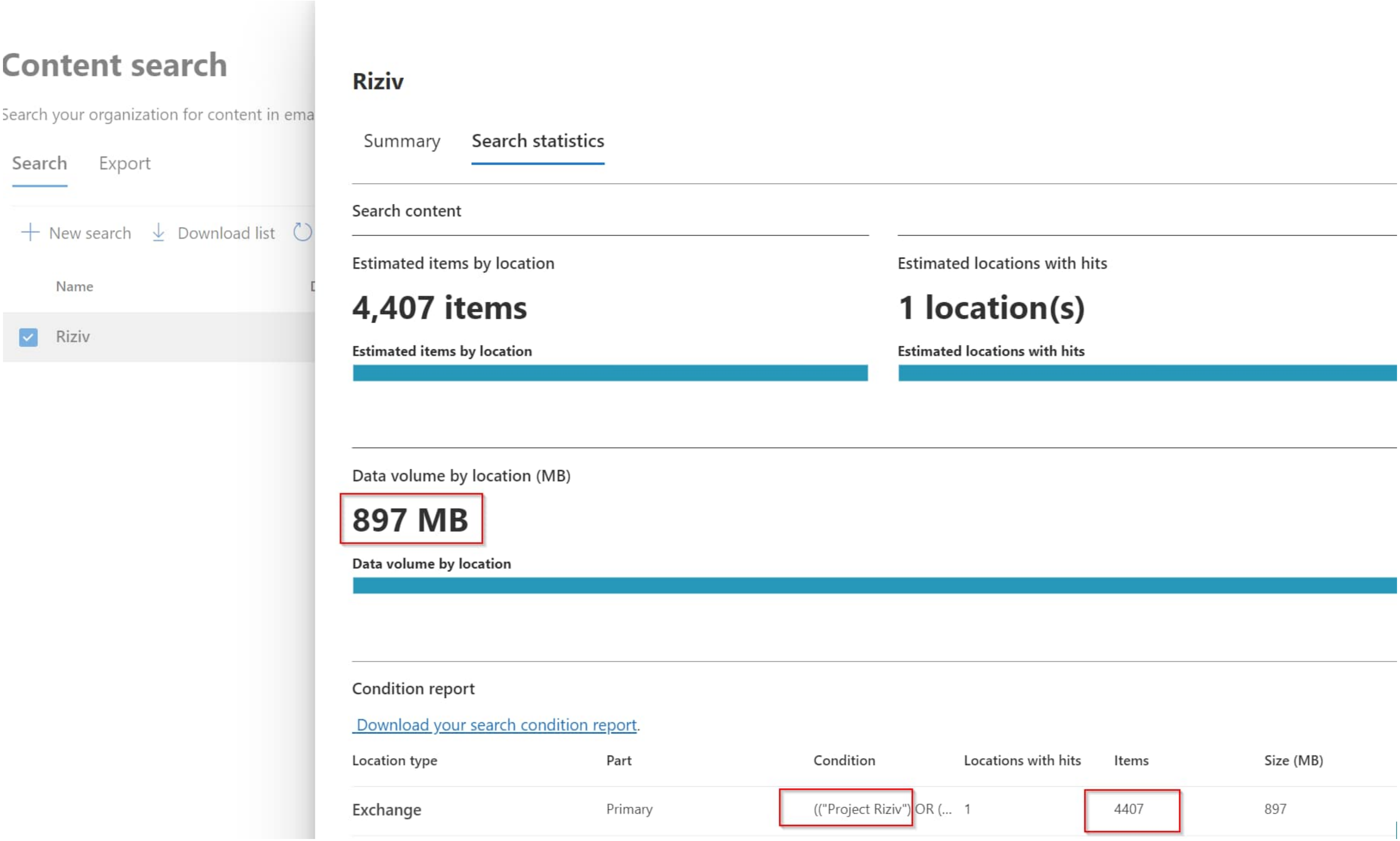
Exchange

Enabled

Exchange public folders

Enabled

Edit locations



Content search

Search your organization for content in ema

Search Export

+ New search ↓ Download list

Name

☑ Riziv

Riziv

Summary Search statistics

Search content

Estimated items by location

4,407 items

Estimated items by location

Estimated locations with hits

1 location(s)

Estimated locations with hits

Data volume by location (MB)

897 MB

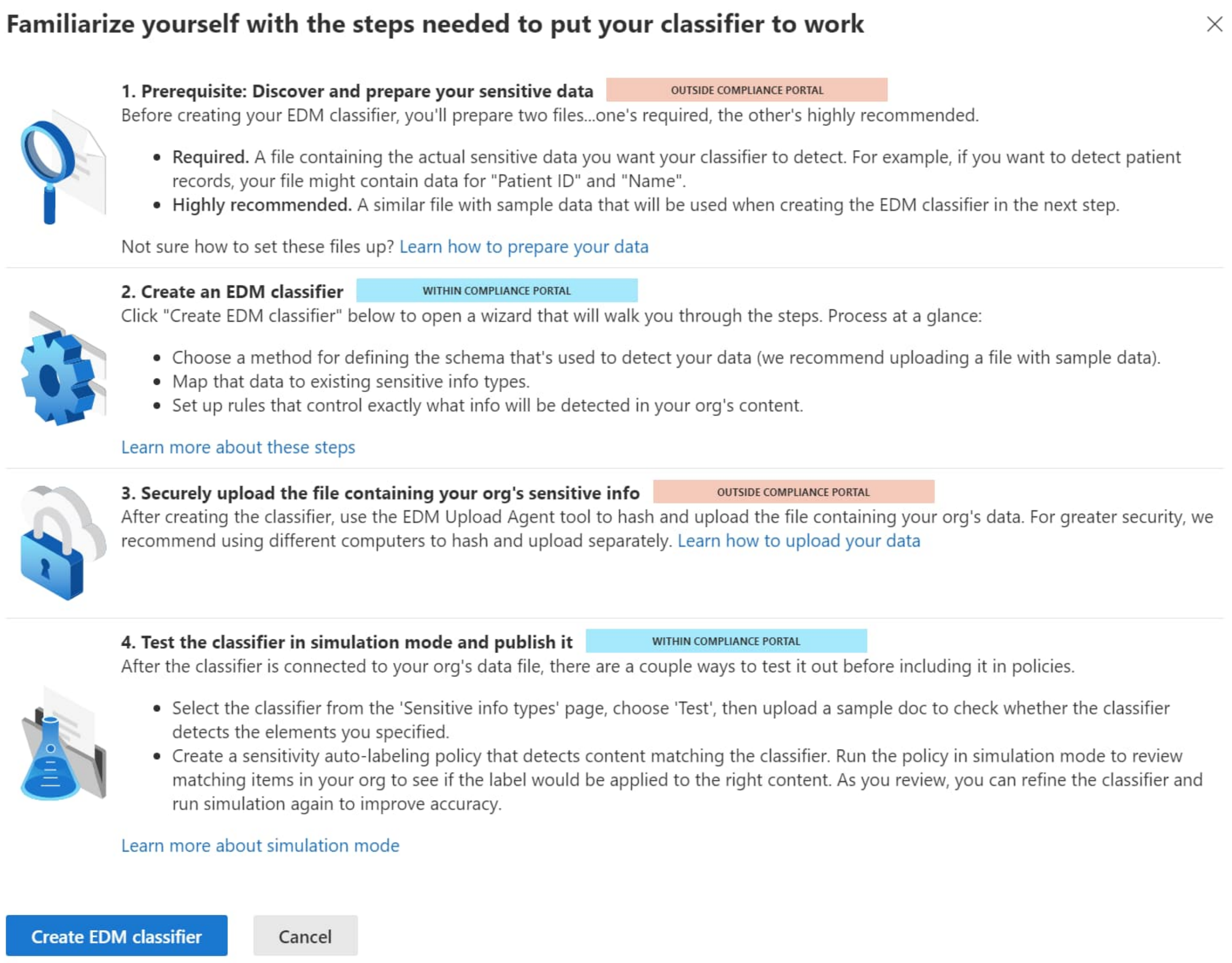
Data volume by location

Condition report

Download your search condition report.

Location type	Part	Condition	Locations with hits	Items	Size (MB)
Exchange	Primary	(("Project Riziv") OR (...	1	4407	897

EDM Classifier



Familiarize yourself with the steps needed to put your classifier to work

1. Prerequisite: Discover and prepare your sensitive data OUTSIDE COMPLIANCE PORTAL

Before creating your EDM classifier, you'll prepare two files...one's required, the other's highly recommended.

- **Required.** A file containing the actual sensitive data you want your classifier to detect. For example, if you want to detect patient records, your file might contain data for "Patient ID" and "Name".
- **Highly recommended.** A similar file with sample data that will be used when creating the EDM classifier in the next step.

Not sure how to set these files up? Learn how to prepare your data

2. Create an EDM classifier WITHIN COMPLIANCE PORTAL

Click "Create EDM classifier" below to open a wizard that will walk you through the steps. Process at a glance:

- Choose a method for defining the schema that's used to detect your data (we recommend uploading a file with sample data).
- Map that data to existing sensitive info types.
- Set up rules that control exactly what info will be detected in your org's content.

Learn more about these steps

3. Securely upload the file containing your org's sensitive info OUTSIDE COMPLIANCE PORTAL

After creating the classifier, use the EDM Upload Agent tool to hash and upload the file containing your org's data. For greater security, we recommend using different computers to hash and upload separately. Learn how to upload your data

4. Test the classifier in simulation mode and publish it WITHIN COMPLIANCE PORTAL

After the classifier is connected to your org's data file, there are a couple ways to test it out before including it in policies.

- Select the classifier from the 'Sensitive info types' page, choose 'Test', then upload a sample doc to check whether the classifier detects the elements you specified.
- Create a sensitivity auto-labeling policy that detects content matching the classifier. Run the policy in simulation mode to review matching items in your org to see if the label would be applied to the right content. As you review, you can refine the classifier and run simulation again to improve accuracy.

Learn more about simulation mode

Thank you!

Q&A

ISACA®

Belgium Chapter

Interplay between NIS and GDPR in Cybersecurity