Evolveum

Preparing for NIS2 Directive Webinar

Peter Pištek, Auditor at Securedo

Radovan Semančík, Co-Founder
and Software Architect at Evolveum

Martin Handl, CEO at Inalogy

Agenda

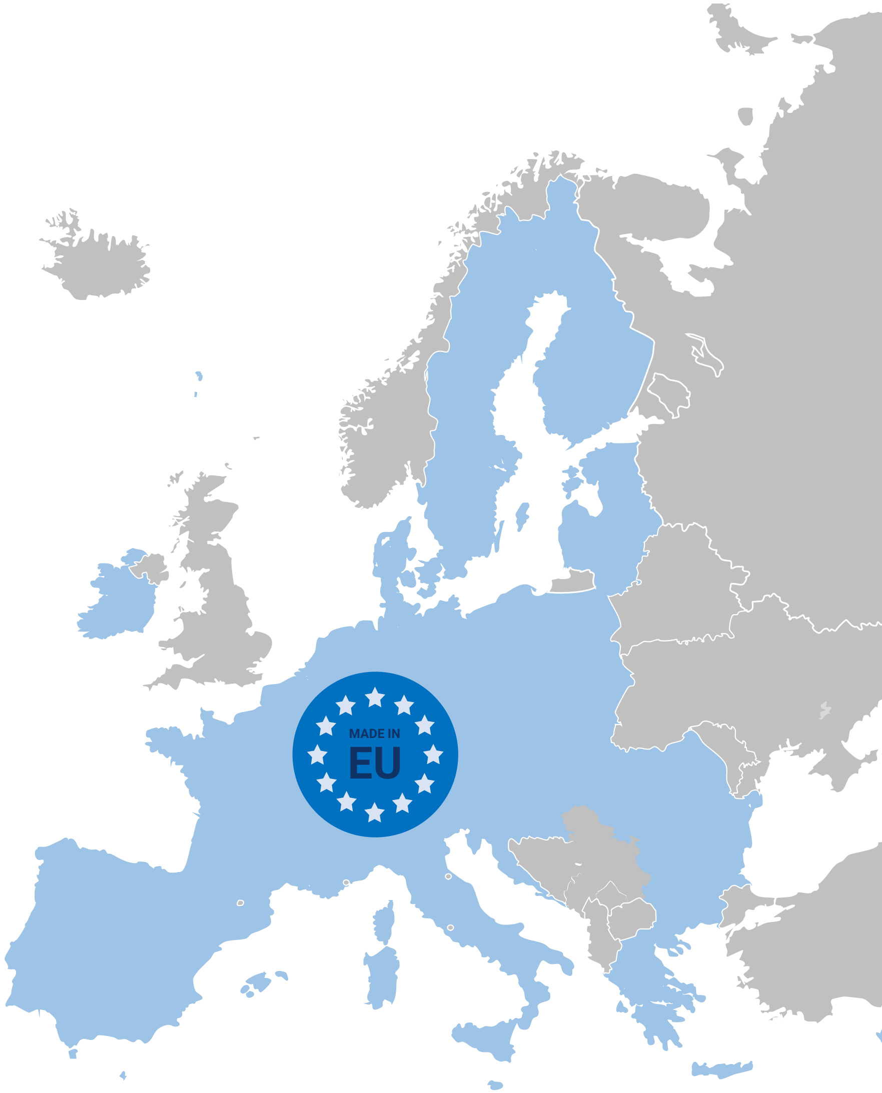
- NIS2 Introduction
  - Peter Pištek (Securedo)
- NIS2 and MidPoint
  - Radovan Semančík (Evolveum)
- Demo
  - Martin Handl (Inalogy)

NIS2 Introduction

What is NIS2

NIS2 Introduction

- EU directive
    - On measures for a high common level of cybersecurity across the European Union
- Must be adopted by the Member States



NIS (2016/1148) vs. NIS2 (2022/2555)

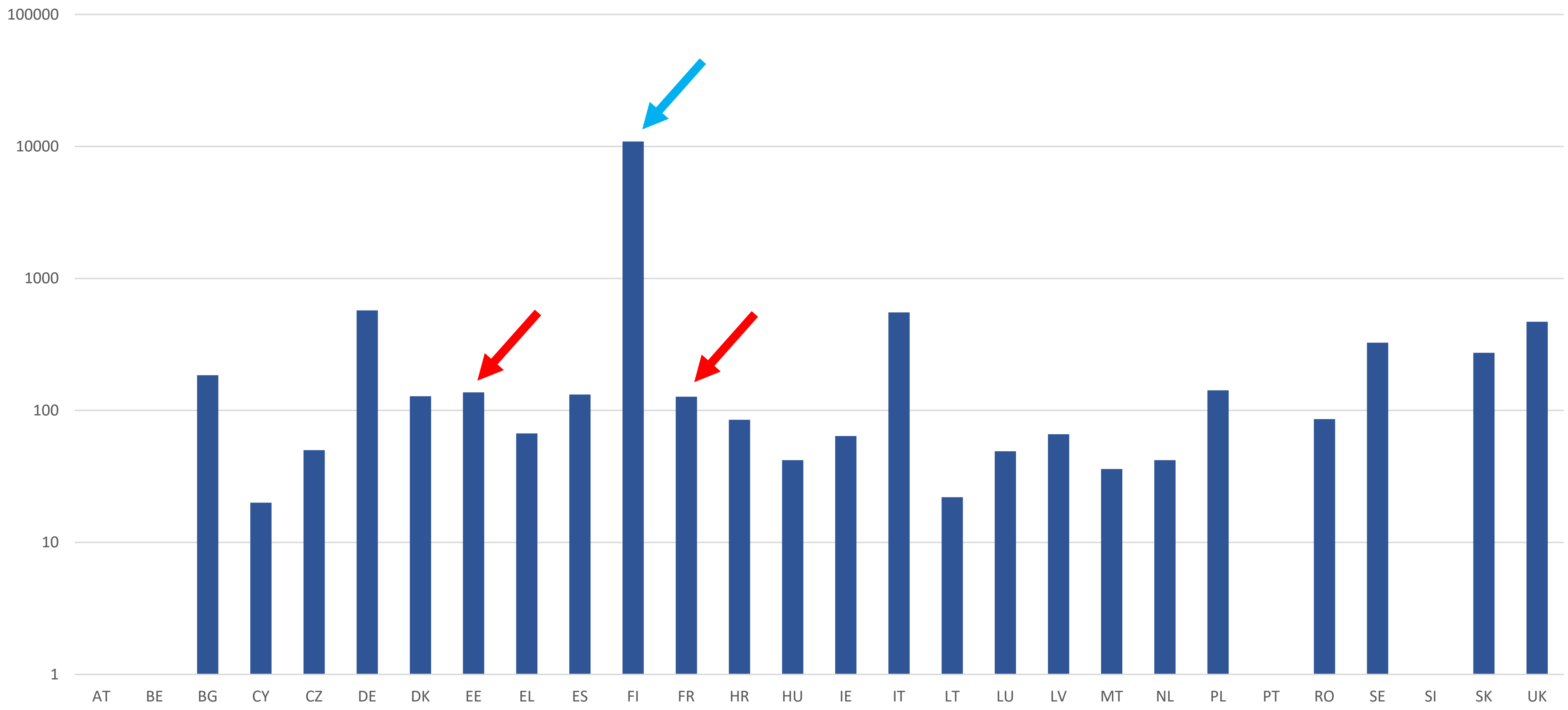
NIS2 Introduction

- Different approaches
  - Type of requirement
  - Level of details
  - Method of supervision
  - Fragmentation of the internal market
- Identification criteria
- Eliminate the wide divergences among Member States

NIS2 – Recitals 4,5,7

Example – Operators of Essential Services (2019)

NIS2 Introduction



https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546

Example – in Detail (2023)

NIS2 Introduction

Country	Population	GDP - nominal ($)	GDP per capita ($)	SME	Large enterprise	NIS entities
Austria	~ 9 mil.	~526 bln $	58 013	~ 330 000	~1 200	136
Czech republic	~ 10,1 mil.	~335 bln $	30 474	~ 1 000 000	~1 608	~400
Slovak republic	~ 5,5 mil.	~145 bln $	26 710	~ 500 000	~ 550	~1800

https://stats.oecd.org/index.aspx?queryid=81354
Wikipedia
KCCKB

NIS2 Entities

NIS2 Introduction

- Entities
  - Essential
    - Regular controls (audits, inspections)
  - Important
    - Provided with evidence, **indication** or information that an entity **allegedly** does not comply with this Directive
- Operator of essential services (NIS) = Essential subject (NIS2)
- Special focus on SMEs and their needs
  - Supply chain
  - Free tools, knowledge, resources

NIS2 (Recital 17, Article 32-33)

NIS2 Entities - Thresholds

NIS2 Introduction

- 50 employees
- 10 million Euros annual turnover
- Specific sector (18)
- Exceptions
  - All entities in selected sector
  - Sole provider of critical services
- Public administration entities at local level
- Education institutions (research)
- Indirect
  - Suppliers

NIS2 (Article 2)

Essential Subjects

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Digital infrastructure
- Drinking water
- Waste water
- ICT service management
- Public administration
- Space

Important Subjects

- Postal and courier services
- Waste management
- Manufacture, production and distribution of chemicals
- Production, processing and distribution of food
- Digital providers
- Research
- Manufacturing*

*Healthcare, electrical equipment, machines, computer, electronic and optical products, motor vehicles, means of transport

NIS2 – Responsibilities

NIS2 Introduction

- **Management bodies** of essential and important entities
  - Oversee implementation of NIS2
  - Can be held liable for infringements

NIS2 (Article 20)

Sanctions

NIS2 Introduction

- **Prohibit** temporarily **chief executive officer** or legal representative level in the essential entity from **exercising managerial functions** in that entity
- Suspend temporarily a certification of all the relevant services
  - EUCC, EUCS, EU5G, AIA
- 10 000 000 €, 2% of total worldwide annual turnover
- 7 000 000 €, 1,4% of total worldwide annual turnover
- Periodic penalty payments

NIS2 (Article 32:5-8, Article 33:5, Article 34)
https://certification.enisa.europa.eu

Deadlines

NIS2 Introduction

- By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive.
  - National legislation
    - 6 month(SK)/1 year (CZ) to be compliant
    - 2026 audit of new entities (SK)

NIS2 (Article 41, Article 3)

Measures

NIS2 Introduction

a) Policies on risk analysis and information system security;

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 cyber 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 communication systems within the entity, where appropriate.

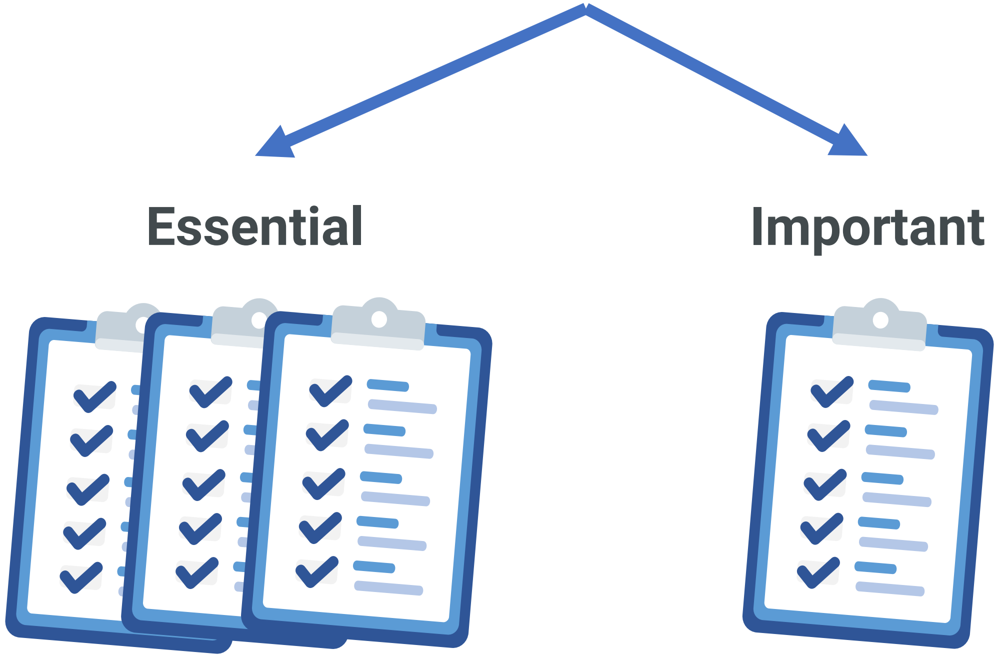
NIS2 (Article 21)

Measures

NIS2 Introduction

NIS2 -> ISO/IEC 27000(2)

What? How?



Essential

Important

NIS2 (Recitals 59, 79, 80)

NIS2 and MidPoint

NIS2: Article 21, Paragraph 2

NIS2 and MidPoint

... shall include at least the following:

- *(a) policies on risk analysis and information system security;*
- ***(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 cyber 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 communication systems within the entity, where appropriate.*

NIS2: Technical Requirements

NIS2 and MidPoint

- NIS2 is a legislation (EU directive) => it is technically vague
- Article 21, paragraph 2: the only “technical” specification
    - Note: AIM is part of cyberhygiene [Recital 89]
- Further details in national law, implementing acts (if any), or sector-specific regulation (CER, DORA, ...)
- International standards to the rescue

IGA Features for NIS2

NIS2 and MidPoint

WARNING: No **product** can be NIS2 compliant, or make you NIS2 compliant. Compliance is responsibility of each **organization**.

- Identity lifecyle, synchronization, provisioning (cyberhygiene)
- Access control (RBAC, entitlements)
- Reporting (policies, demostrating compliance)
- Audit trail (incident handling, reporting obligations)
- Application inventory (asset management)
- Credential management, provisioning (authentication)

Disclaimer: lot of guesswork involved

Proportionality and Standardization

NIS2 and MidPoint

- "... ***appropriate and proportionate*** *technical, operational and organisational measures … taking into account the* ***state-of-the-art*** *and, where applicable, relevant* ***European and international standards****, as well as the cost of implementation …”*
  [Article 21, paragraph 1]
- Strong focus on **best practice** and **standardization**
  [Recital 58] [Recital 59] [Recital 79] [Recital 81] [Article 21] [Article 25]
- ISO 27000 explicitly mentioned
  [Recital 79]
- Proportional → risk-based
- Bottom line: Manage your cybersecurity properly and you will be fine

Interesting NIS2 Aspects

NIS2 and MidPoint

- Ecourages use of **innovative technology**, including AI
  [Recital 51]
- Encorages use of **open source**
  [Recital 52]
- Encorages **proportional**, yet **state-of-the-art** measures
  [Recital 81]
- Explicitly mentions **IAM**
  [Recital 89]

NIS2 Implications for MidPoint Development

NIS2 and MidPoint

● Open source	**DONE**
● Proportional	**DONE**
● State of the art	**DONE**
● Innovative technology & AI	**IN PROGRESS**

Evolveum

Our Approach to Compliance

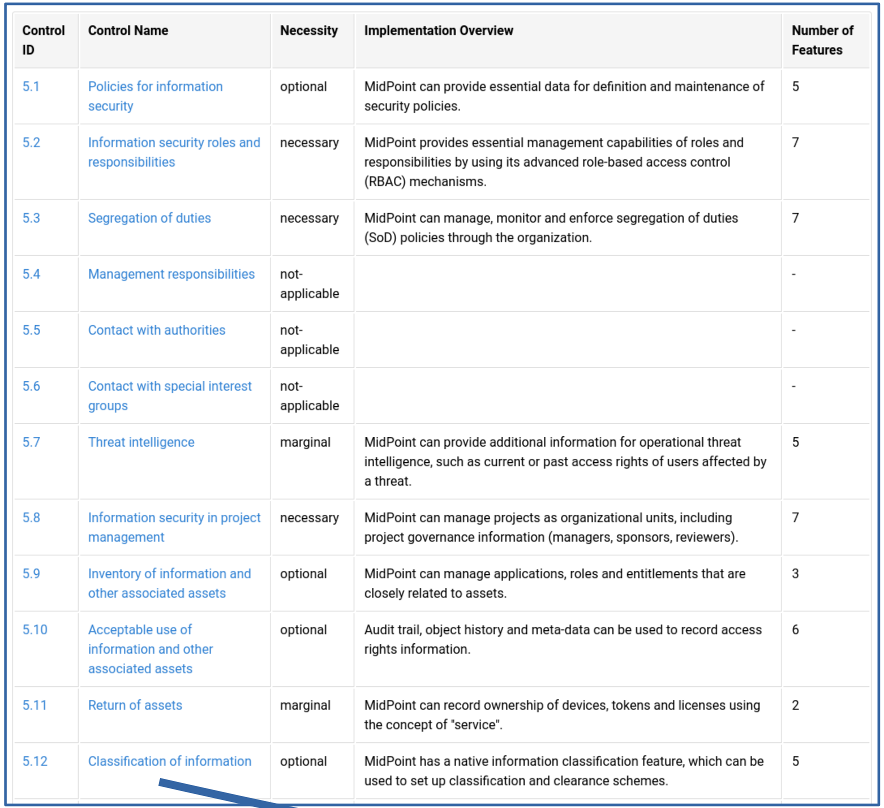
NIS2 and MidPoint

- No product can make you compliant, not even midPoint
- However, midPoint is an essential part of compliance
- How we can help:
  - Statement of Applicability (SoA) information
  - Recommendations for midPoint configuration
  - Documentation
  - Future: Built-in tooling (e.g. compliance checklists/dashboards)

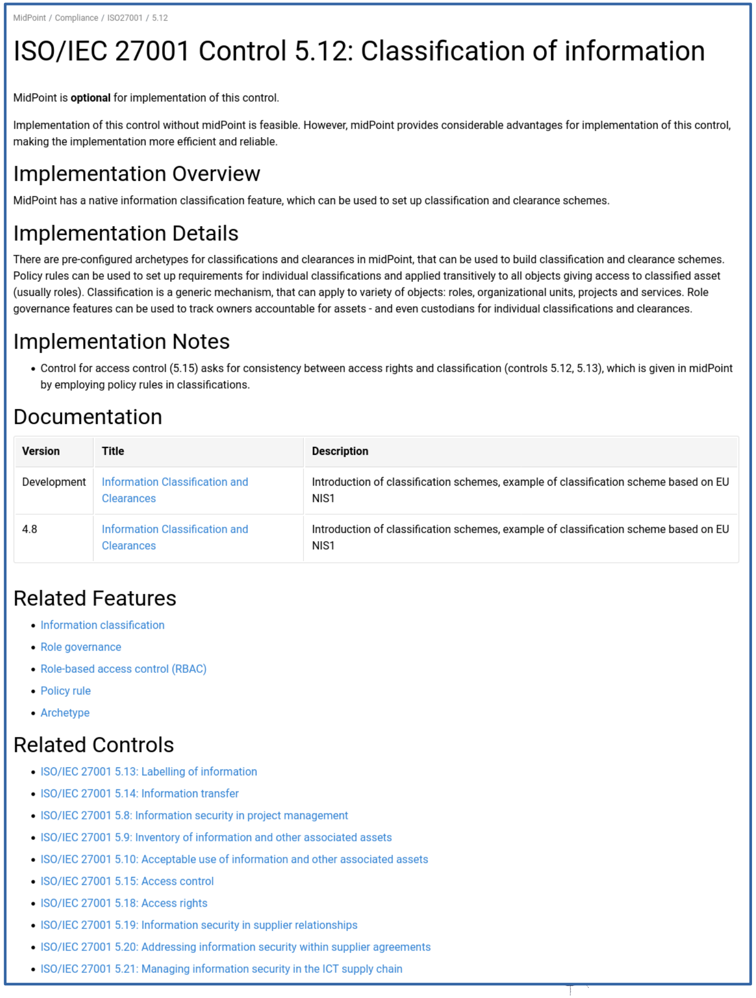
ISO 27001 Compliance with MidPoint

NIS2 and MidPoint

https://docs.evolveum.com/midpoint/compliance/iso27001/



Control ID	Control Name	Necessity	Implementation Overview	Number of Features
5.1	Policies for information security	optional	MidPoint can provide essential data for definition and maintenance of security policies.	5
5.2	Information security roles and responsibilities	necessary	MidPoint provides essential management capabilities of roles and responsibilities by using its advanced role-based access control (RBAC) mechanisms.	7
5.3	Segregation of duties	necessary	MidPoint can manage, monitor and enforce segregation of duties (SoD) policies through the organization.	7
5.4	Management responsibilities	not-applicable		-
5.5	Contact with authorities	not-applicable		-
5.6	Contact with special interest groups	not-applicable		-
5.7	Threat intelligence	marginal	MidPoint can provide additional information for operational threat intelligence, such as current or past access rights of users affected by a threat.	5
5.8	Information security in project management	necessary	MidPoint can manage projects as organizational units, including project governance information (managers, sponsors, reviewers).	7
5.9	Inventory of information and other associated assets	optional	MidPoint can manage applications, roles and entitlements that are closely related to assets.	3
5.10	Acceptable use of information and other associated assets	optional	Audit trail, object history and meta-data can be used to record access rights information.	6
5.11	Return of assets	marginal	MidPoint can record ownership of devices, tokens and licenses using the concept of "service".	2
5.12	Classification of information	optional	MidPoint has a native information classification feature, which can be used to set up classification and clearance schemes.	5



MidPoint / Compliance / ISO27001 / 5.12

ISO/IEC 27001 Control 5.12: Classification of information

MidPoint is **optional** for implementation of this control.

Implementation of this control without midPoint is feasible. However, midPoint provides considerable advantages for implementation of this control, making the implementation more efficient and reliable.

Implementation Overview

MidPoint has a native information classification feature, which can be used to set up classification and clearance schemes.

Implementation Details

There are pre-configured archetypes for classifications and clearances in midPoint, that can be used to build classification and clearance schemes. Policy rules can be used to set up requirements for individual classifications and applied transitively to all objects giving access to classified asset (usually roles). Classification is a generic mechanism, that can apply to variety of objects: roles, organizational units, projects and services. Role governance features can be used to track owners accountable for assets - and even custodians for individual classifications and clearances.

Implementation Notes

- Control for access control (5.15) asks for consistency between access rights and classification (controls 5.12, 5.13), which is given in midPoint by employing policy rules in classifications.

Documentation

Version	Title	Description
Development	Information Classification and Clearances	Introduction of classification schemes, example of classification scheme based on EU NIS1
4.8	Information Classification and Clearances	Introduction of classification schemes, example of classification scheme based on EU NIS1

Related Features

- Information classification
- Role governance
- Role-based access control (RBAC)
- Policy rule
- Archetype

Related Controls

- ISO/IEC 27001 5.13: Labelling of information
- ISO/IEC 27001 5.14: Information transfer
- ISO/IEC 27001 5.8: Information security in project management
- ISO/IEC 27001 5.9: Inventory of information and other associated assets
- ISO/IEC 27001 5.10: Acceptable use of information and other associated assets
- ISO/IEC 27001 5.15: Access control
- ISO/IEC 27001 5.18: Access rights
- ISO/IEC 27001 5.19: Information security in supplier relationships
- ISO/IEC 27001 5.20: Addressing information security within supplier agreements
- ISO/IEC 27001 5.21: Managing information security in the ICT supply chain

Demo

Conclusion

- NIS2 harmonizes EU **cybersecurity legislation**
- NIS2 is **technically vague** (EU directive)
- Focus on **international standards** and best practice:
  ISO 27000 series, NIST CSF, …
- **IAM** is an essential part of the solution
- **MidPoint** has features to support NIS2 compliance
- Evolveum **partners** are here to help with local knowledge

Upcoming Webinars

- Introduction to Flexible Authentication (May 16, 2024)
- ISO27001 Compliance with MidPoint (May 30, 2024)
- Teaser: MidPoint Deployment Intermediate Configuration Training (Jun 20, 2024)

Thank you for your attention

Do you have any **questions**? Feel free to contact us at **info@evolveum.com**

Follow us on social media or **join us** at GitHub or Gitter!

/Evolveum

@Evolveum

/Evolveum

/Evolveum

/Evolveum

Evolveum