Evolveum

ISO 27001 Directive Webinar

Peter Pištek, Auditor at Securedo

Radovan Semančík, Co-Founder
and Software Architect at Evolveum

Agenda

- ISO Introduction
  - Peter Pištek (Securedo)
- NIS2 and MidPoint
  - Radovan Semančík (Evolveum)

ISO/IEC 27001 Introduction

Evolveum

ISO/IEC 27001

Introduction

- International standard
  - Any size, all sectors
- Risk based approach
- Note: ISO/IEC 27001:2022 -> ISO 27001

ISO 27001 Certification Process 101

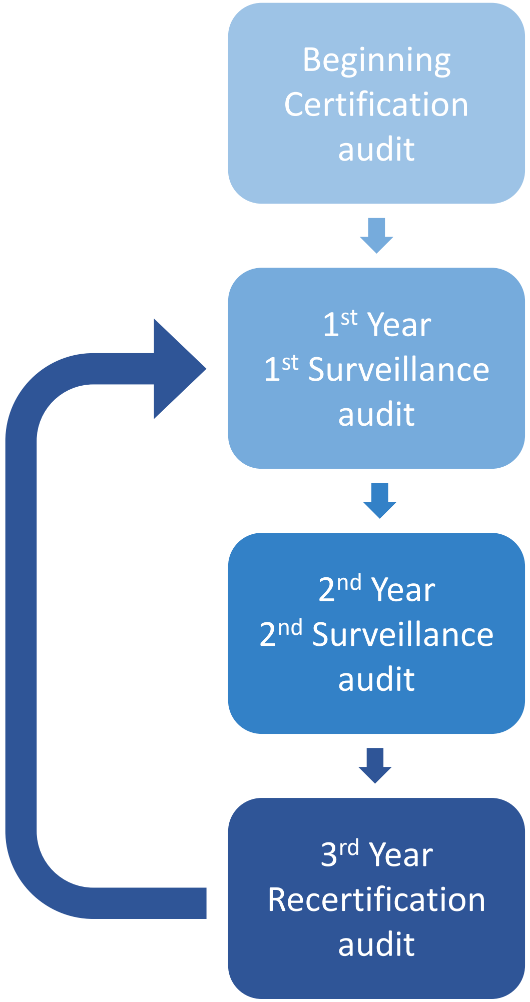
Before Certification

- Certification decision
  - Create project plan
  - Define scope of your ISMS
- GAP analysis of current state vs ISO 27001 requirements
- Implementation of ISO 27001 requirements
- Internal audit / preliminary audit

ISO 27001 Certification Process 101

Continuous Compliance

- Certification audit
  - System analysis / Design review (documentation)
  - System evaluation (implementation)
- Results
- Continuous compliance
  - Internal audits
  - Surveillance audits
- Recertification audit



Beginning Certification audit

1st Year
1st Surveillance audit

2nd Year
2nd Surveillance audit

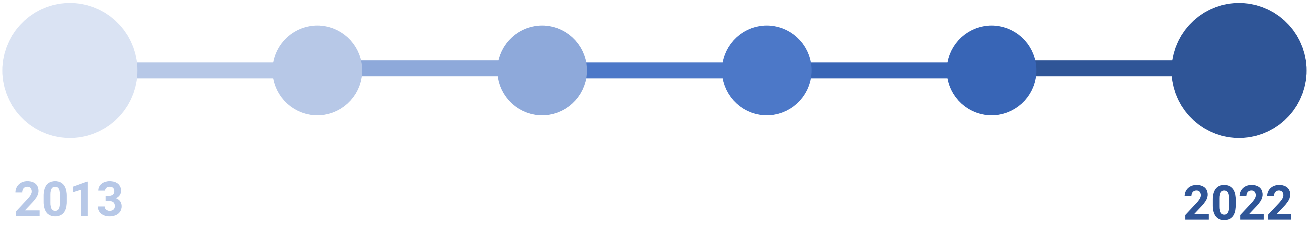
3rd Year
Recertification audit

ISO 27001 2013 -> 2022

Introduction

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

- **Information security**, **cybersecurity** and **privacy** protection — Information security management systems — Requirements



ISO 27001

Introduction

- 93 security controls
- Simplification of risk management
    - one register of controls for information security, cyber security, cloud, and privacy

Domains and Controls

ISO 27001

- 4 domains (93 controls)
  - Organizational (37)
  - People (8)
  - Physical (14)
  - Technical (34)

- “Other” (26)
  - Context of the organization (5)
  - Leadership (3)
  - Planning (5)
  - Support (7)
  - Operation (3)
  - Performance evaluation (3)
  - Improvement (2)

Helpful Guidelines

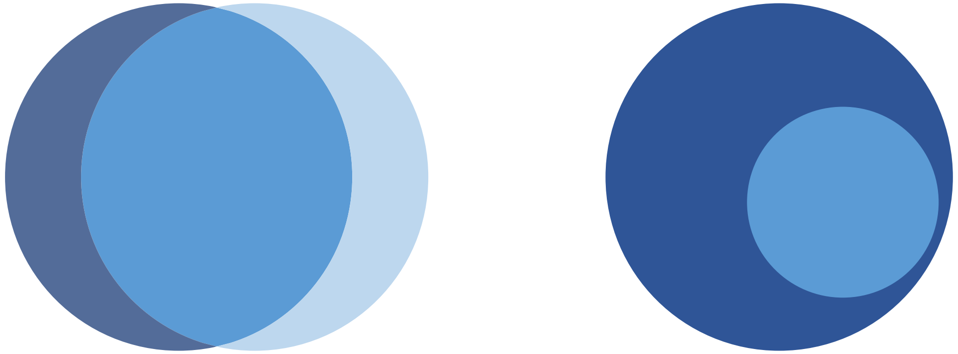
ISO 27000 Family

- **27002**
  - Guidelines to ISO 27001 information security controls and how to implement them
- 27003
  - Implementation of Information security management system according to ISO 27001
- 27004
  - Monitoring, measurement, analysis and evaluation of controls
- 27005
  - Guidance on managing information security risks

ISO 27001 Controls - Reusability

Other Standards, Regulations

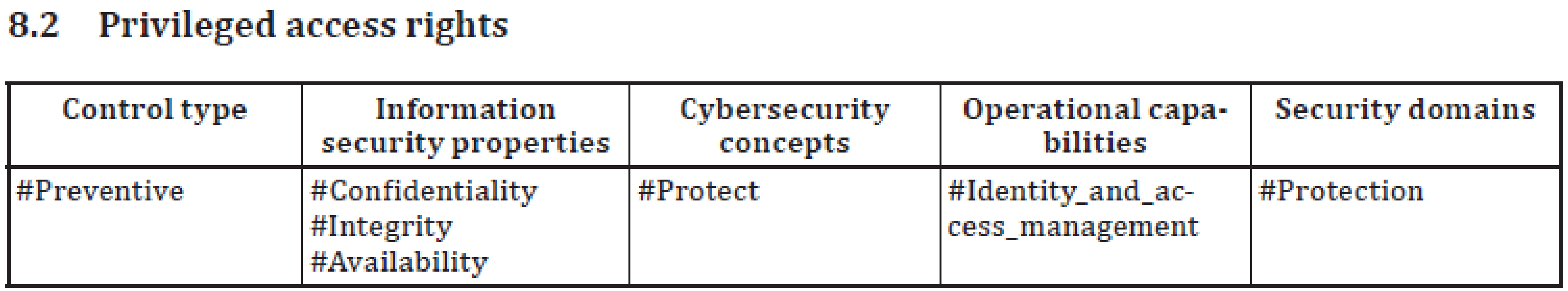
- Technical norm (especially 27002)
- Baseline and inspiration
  - NIST CSF
  - EU directives – NIS, NIS2, DORA, AIA, GDPR
  - PSI DSS, HIPPA
  - …



Analytics

ISO 27002

- #hashtags
  - Maturity level (CMM)
  - Compliance average for category

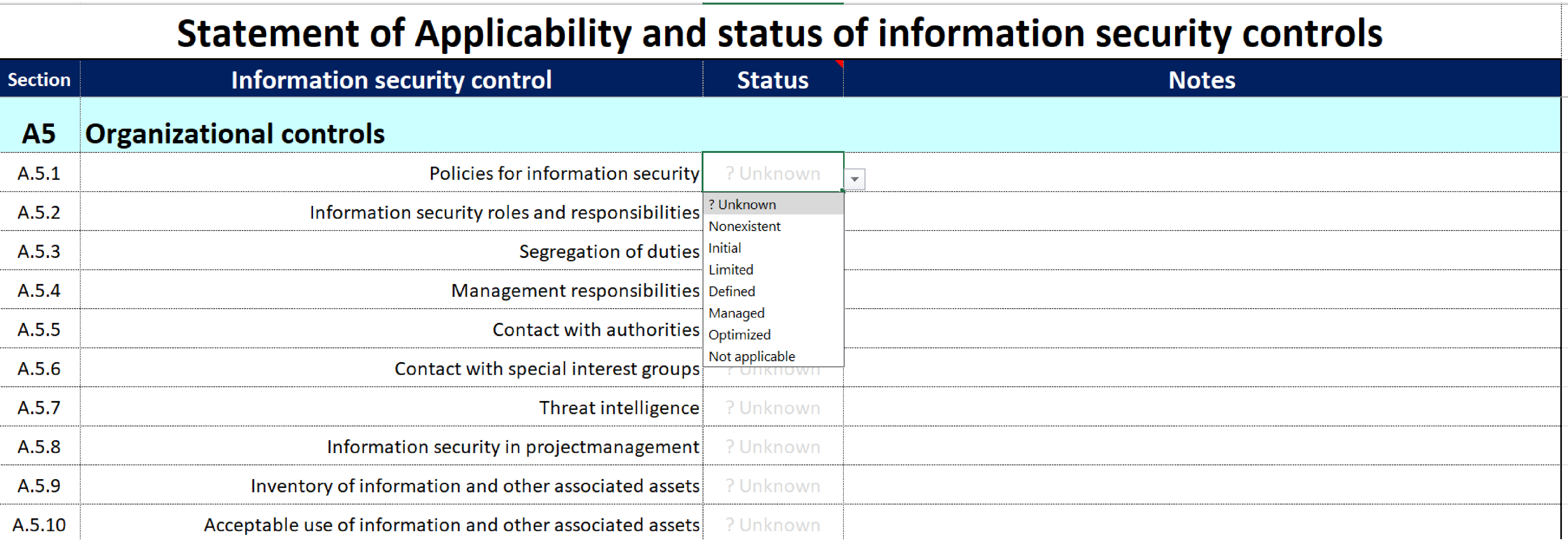


8.2 Privileged access rights

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

ISO 27001 Statement of Applicability

Example



Statement of Applicability and status of information security controls

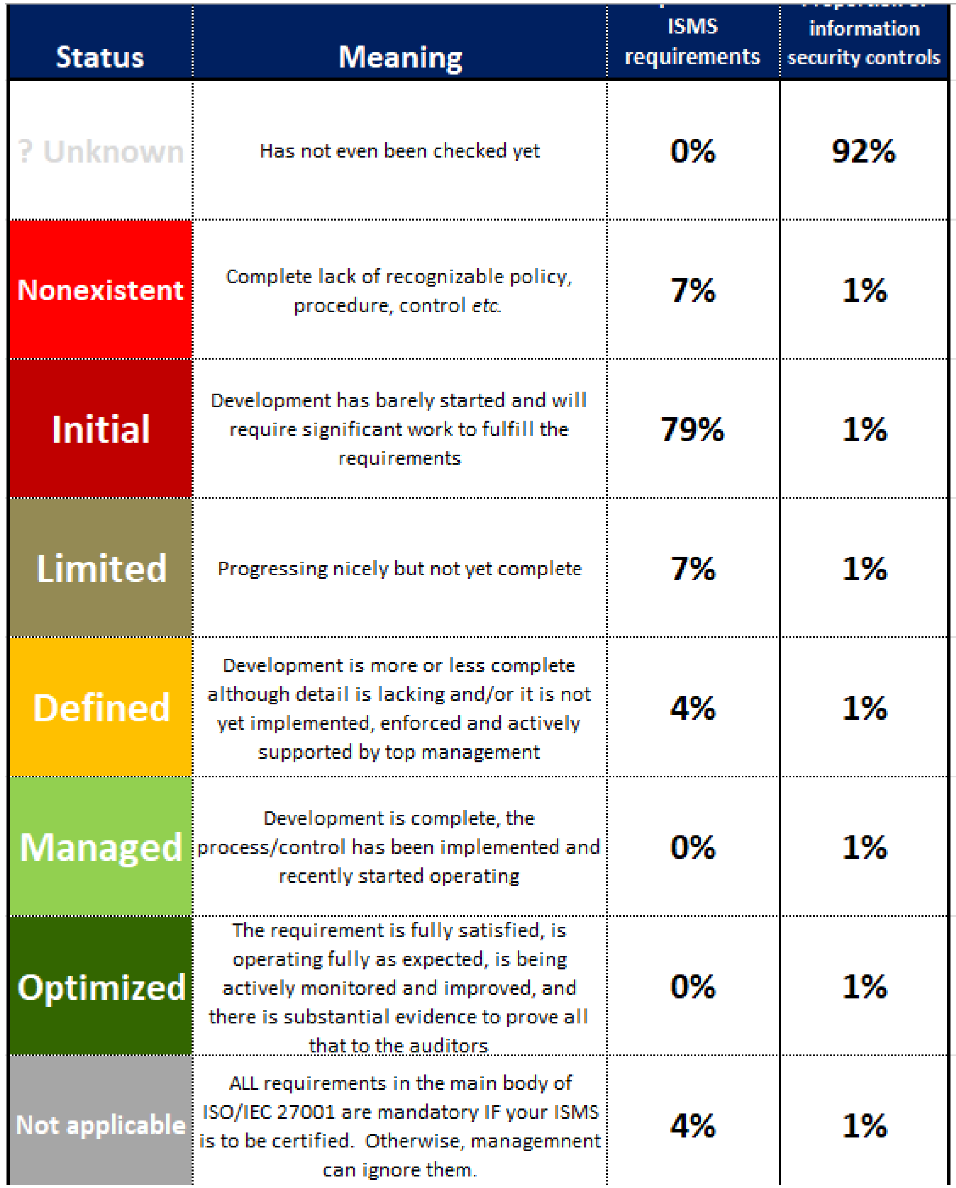
Section	Information security control	Status	Notes
A5	**Organizational controls**		
A.5.1	Policies for information security	? Unknown	
A.5.2	Information security roles and responsibilities		
A.5.3	Segregation of duties		
A.5.4	Management responsibilities		
A.5.5	Contact with authorities		
A.5.6	Contact with special interest groups	? Unknown	
A.5.7	Threat intelligence	? Unknown	
A.5.8	Information security in projectmanagement	? Unknown	
A.5.9	Inventory of information and other associated assets	? Unknown	
A.5.10	Acceptable use of information and other associated assets	? Unknown	

https://www.iso27001security.com/

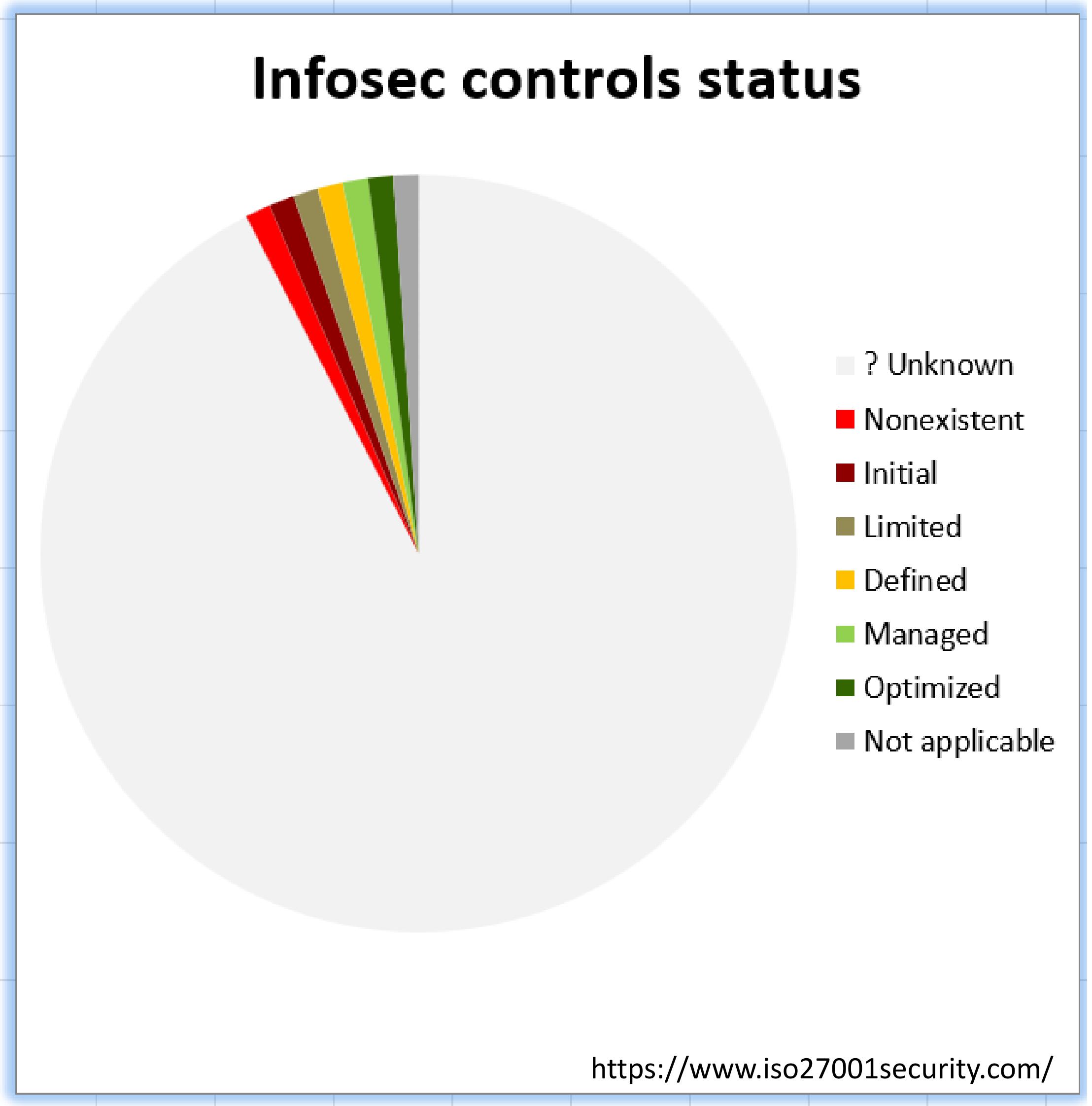
Evolveum

ISO 27001 Statement of Applicability

Maturity



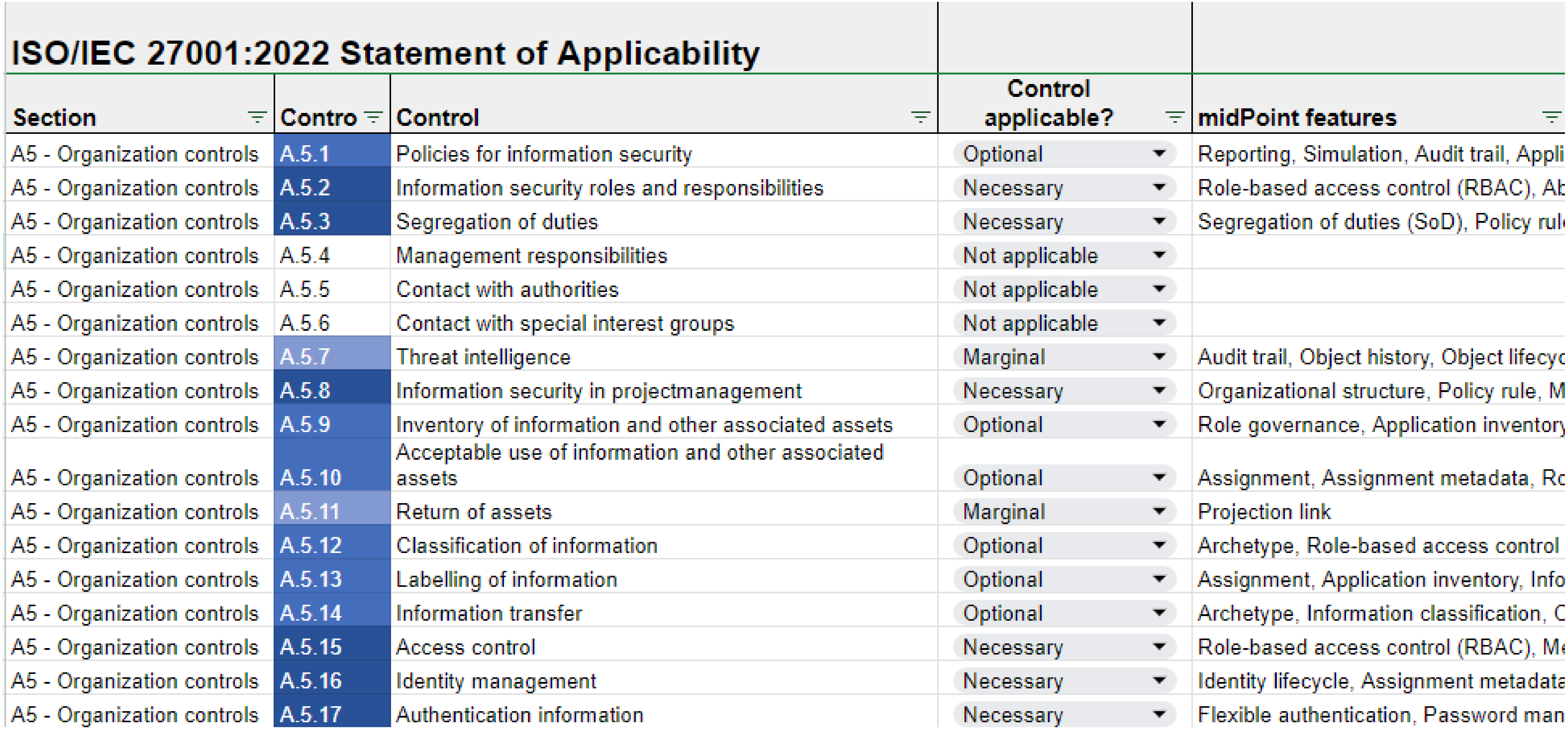
Status	Meaning	ISMS requirements	information security controls
? Unknown	Has not even been checked yet	0%	92%
Nonexistent	Complete lack of recognizable policy, procedure, control *etc.*	7%	1%
Initial	Development has barely started and will require significant work to fulfill the requirements	79%	1%
Limited	Progressing nicely but not yet complete	7%	1%
Defined	Development is more or less complete although detail is lacking and/or it is not yet implemented, enforced and actively supported by top management	4%	1%
Managed	Development is complete, the process/control has been implemented and recently started operating	0%	1%
Optimized	The requirement is fully satisfied, is operating fully as expected, is being actively monitored and improved, and there is substantial evidence to prove all that to the auditors	0%	1%
Not applicable	ALL requirements in the main body of ISO/IEC 27001 are mandatory IF your ISMS is to be certified. Otherwise, managemnent can ignore them.	4%	1%



https://www.iso27001security.com/

Statement of Applicability – MidPoint Version

Controls

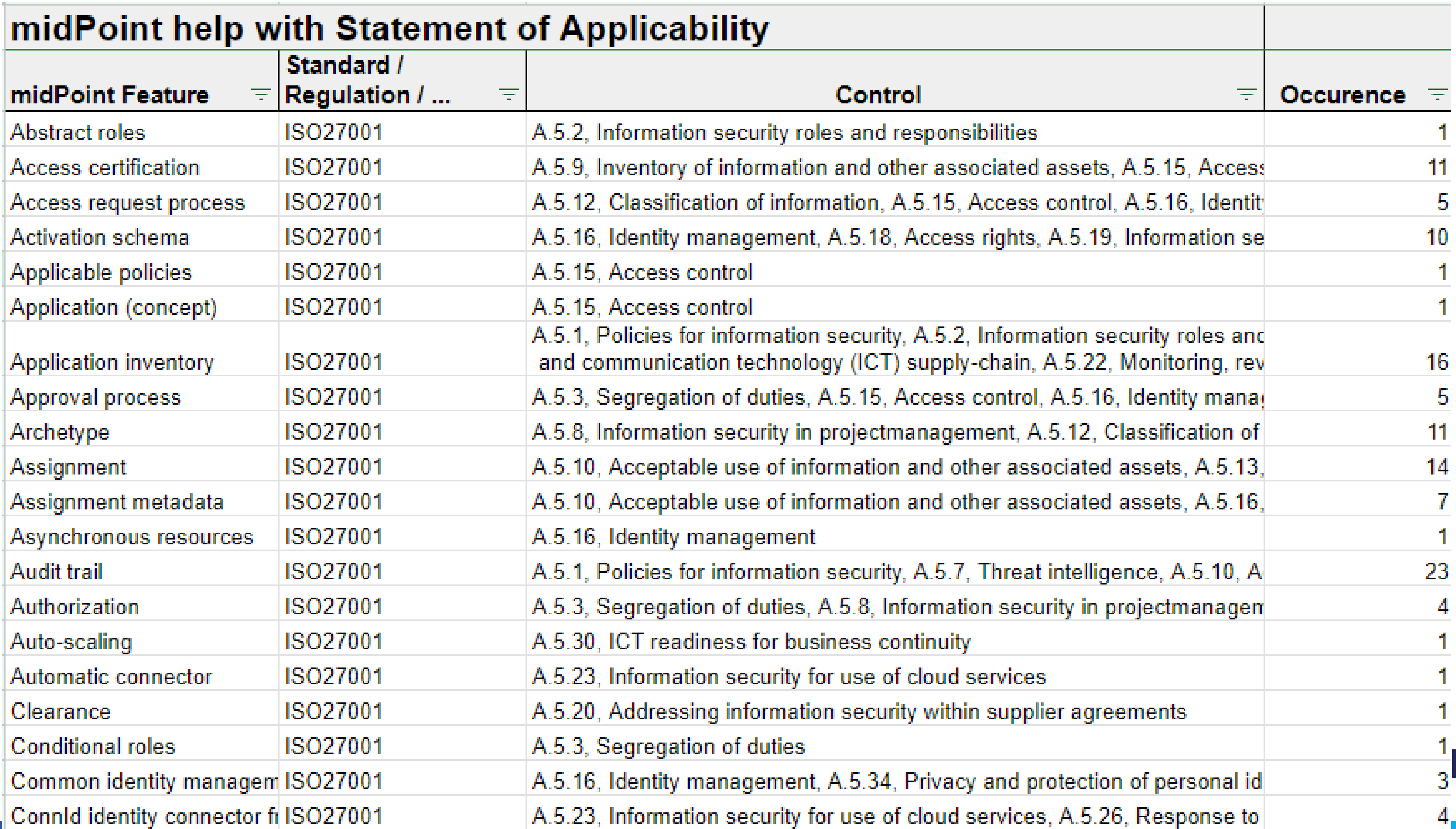


ISO/IEC 27001:2022 Statement of Applicability

Section	Contro	Control	Control applicable?	midPoint features
A5 - Organization controls	A.5.1	Policies for information security	Optional	Reporting, Simulation, Audit trail, Appli
A5 - Organization controls	A.5.2	Information security roles and responsibilities	Necessary	Role-based access control (RBAC), Ab
A5 - Organization controls	A.5.3	Segregation of duties	Necessary	Segregation of duties (SoD), Policy rul
A5 - Organization controls	A.5.4	Management responsibilities	Not applicable	
A5 - Organization controls	A.5.5	Contact with authorities	Not applicable	
A5 - Organization controls	A.5.6	Contact with special interest groups	Not applicable	
A5 - Organization controls	A.5.7	Threat intelligence	Marginal	Audit trail, Object history, Object lifecyc
A5 - Organization controls	A.5.8	Information security in projectmanagement	Necessary	Organizational structure, Policy rule, M
A5 - Organization controls	A.5.9	Inventory of information and other associated assets	Optional	Role governance, Application inventory
A5 - Organization controls	A.5.10	Acceptable use of information and other associated assets	Optional	Assignment, Assignment metadata, Ro
A5 - Organization controls	A.5.11	Return of assets	Marginal	Projection link
A5 - Organization controls	A.5.12	Classification of information	Optional	Archetype, Role-based access control
A5 - Organization controls	A.5.13	Labelling of information	Optional	Assignment, Application inventory, Info
A5 - Organization controls	A.5.14	Information transfer	Optional	Archetype, Information classification, C
A5 - Organization controls	A.5.15	Access control	Necessary	Role-based access control (RBAC), Me
A5 - Organization controls	A.5.16	Identity management	Necessary	Identity lifecycle, Assignment metadata
A5 - Organization controls	A.5.17	Authentication information	Necessary	Flexible authentication, Password man

ISO 27001 Statement of Applicability – MidPoint Version

MidPoint Functionality

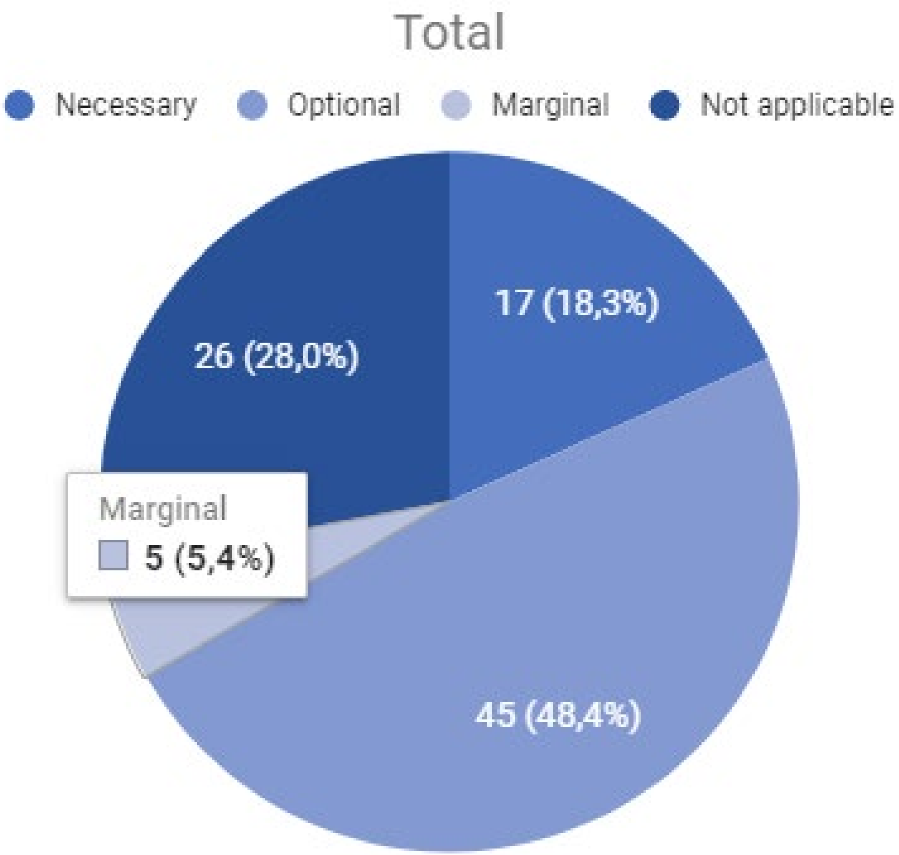


midPoint help with Statement of Applicability

midPoint Feature	Standard / Regulation / ...	Control	Occurence
Abstract roles	ISO27001	A.5.2, Information security roles and responsibilities	1
Access certification	ISO27001	A.5.9, Inventory of information and other associated assets, A.5.15, Access	11
Access request process	ISO27001	A.5.12, Classification of information, A.5.15, Access control, A.5.16, Identit	5
Activation schema	ISO27001	A.5.16, Identity management, A.5.18, Access rights, A.5.19, Information se	10
Applicable policies	ISO27001	A.5.15, Access control	1
Application (concept)	ISO27001	A.5.15, Access control	1
Application inventory	ISO27001	A.5.1, Policies for information security, A.5.2, Information security roles anc and communication technology (ICT) supply-chain, A.5.22, Monitoring, rev	16
Approval process	ISO27001	A.5.3, Segregation of duties, A.5.15, Access control, A.5.16, Identity mana	5
Archetype	ISO27001	A.5.8, Information security in projectmanagement, A.5.12, Classification of	11
Assignment	ISO27001	A.5.10, Acceptable use of information and other associated assets, A.5.13,	14
Assignment metadata	ISO27001	A.5.10, Acceptable use of information and other associated assets, A.5.16,	7
Asynchronous resources	ISO27001	A.5.16, Identity management	1
Audit trail	ISO27001	A.5.1, Policies for information security, A.5.7, Threat intelligence, A.5.10, A	23
Authorization	ISO27001	A.5.3, Segregation of duties, A.5.8, Information security in projectmanagem	4
Auto-scaling	ISO27001	A.5.30, ICT readiness for business continuity	1
Automatic connector	ISO27001	A.5.23, Information security for use of cloud services	1
Clearance	ISO27001	A.5.20, Addressing information security within supplier agreements	1
Conditional roles	ISO27001	A.5.3, Segregation of duties	1
Common identity managem	ISO27001	A.5.16, Identity management, A.5.34, Privacy and protection of personal id	3
ConnId identity connector fi	ISO27001	A.5.23, Information security for use of cloud services, A.5.26, Response to	4

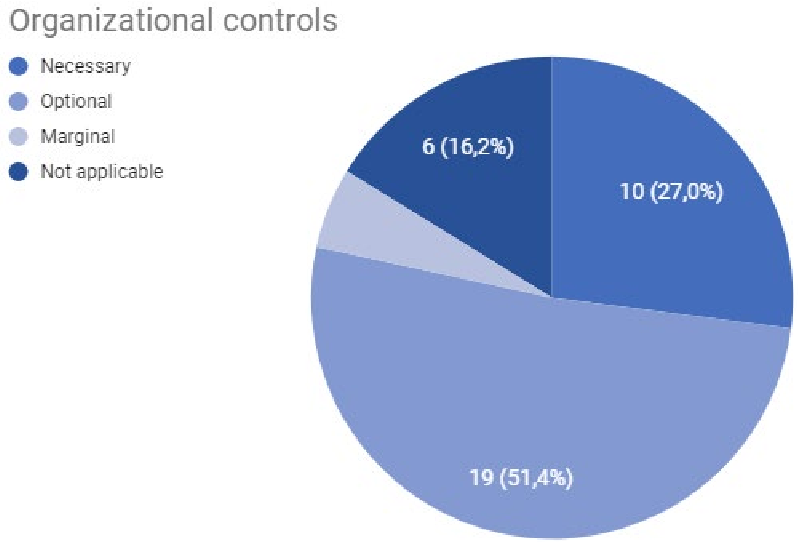
ISO 27001 Statement of Applicability

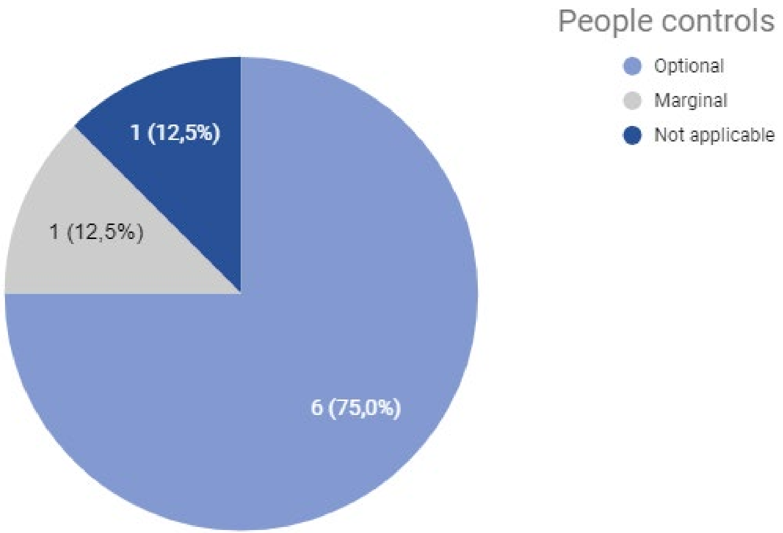
All Controls

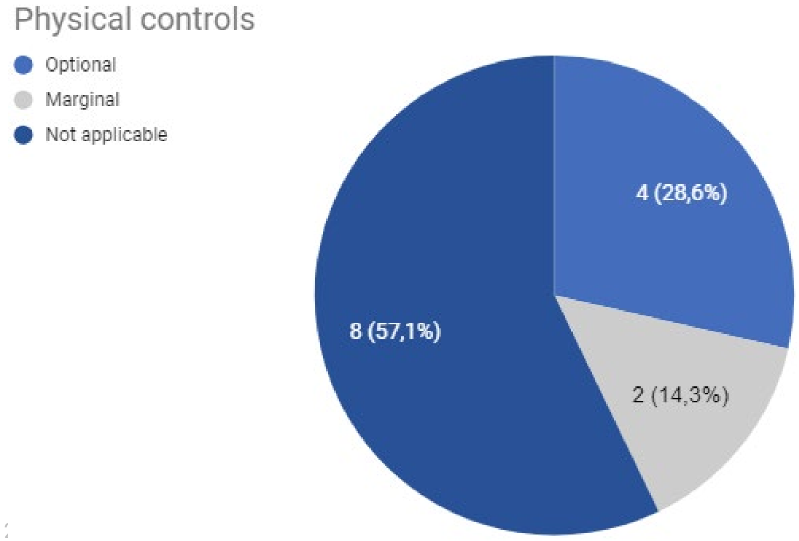


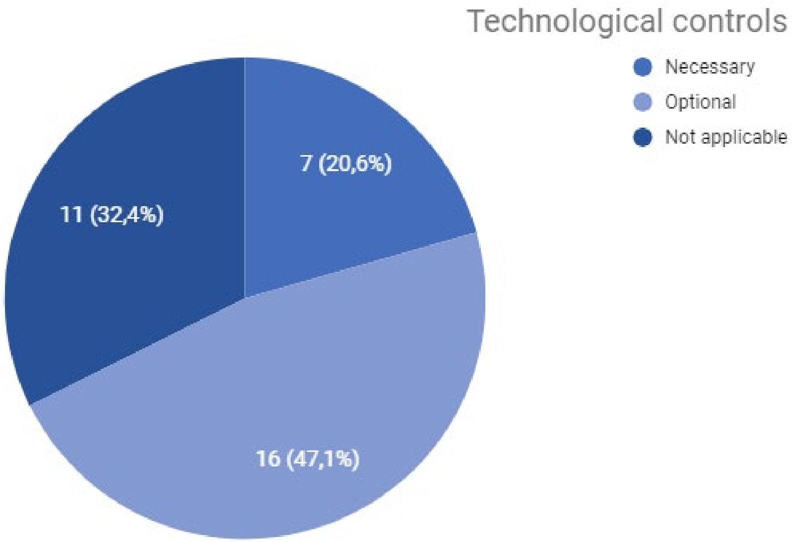
ISO 27001 Statement of Applicability

Per Domain


Organizational controls


People controls


Physical controls


Technological controls

ISO/IEC 27000 Series and MidPoint

Overview

ISO 27000 and MidPoint

WARNING: No **product** can be ISO 27001 compliant, or make you ISO 27001 compliant. Compliance is responsibility of each **organization**.

What are we doing to help you with ISO 27001 compliance?

- ISO/IEC 27000 glossary
  https://docs.evolveum.com/glossary/iso27000/
- Documenting ISO/IEC 27001 controls
  https://docs.evolveum.com/midpoint/compliance/iso27001/
- Statements of Applicability (SOA)
- New features and improvements (midPoint 4.9+)
  https://docs.evolveum.com/midpoint/roadmap/

Documenting ISO/IEC 27001 Controls

ISO 27000 and MidPoint

Work in progress

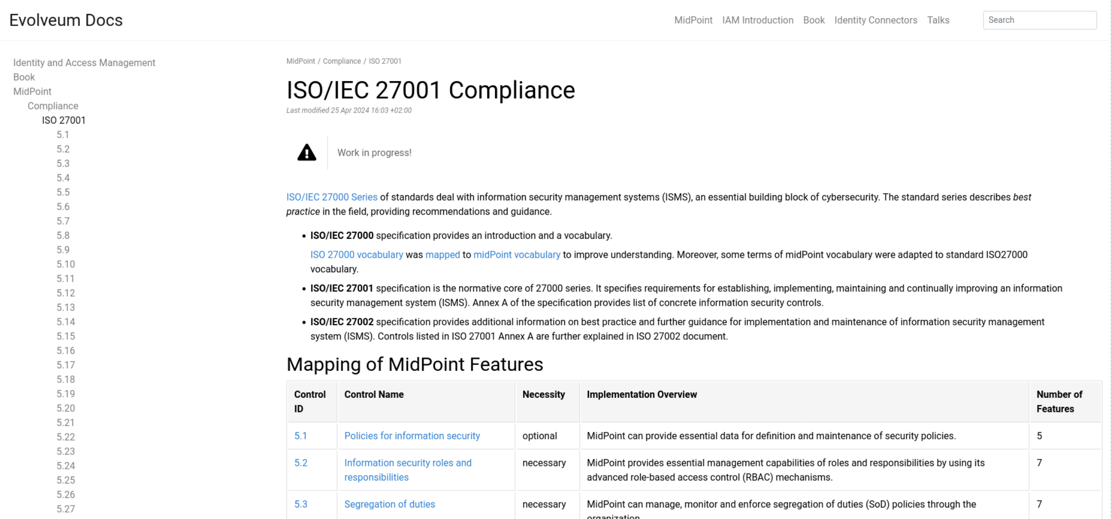
https://docs.evolveum.com/midpoint/compliance/iso27001/

docs.evolveum.com

↳ MidPoint

↳ Compliance

↳ ISO 27001



Evolveum Docs

MidPoint IAM Introduction Book Identity Connectors Talks Search

Identity and Access Management
Book
MidPoint
Compliance
ISO 27001
5.1
5.2
5.3
5.4
5.5
5.6
5.7
5.8
5.9
5.10
5.11
5.12
5.13
5.14
5.15
5.16
5.17
5.18
5.19
5.20
5.21
5.22
5.23
5.24
5.25
5.26
5.27

MidPoint / Compliance / ISO 27001

ISO/IEC 27001 Compliance

Last modified 25 Apr 2024 16:03 +02:00

Work in progress!

ISO/IEC 27000 Series of standards deal with information security management systems (ISMS), an essential building block of cybersecurity. The standard series describes *best practice* in the field, providing recommendations and guidance.

- **ISO/IEC 27000** specification provides an introduction and a vocabulary.

  ISO 27000 vocabulary was mapped to midPoint vocabulary to improve understanding. Moreover, some terms of midPoint vocabulary were adapted to standard ISO27000 vocabulary.
- **ISO/IEC 27001** specification is the normative core of 27000 series. It specifies requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS). Annex A of the specification provides list of concrete information security controls.
- **ISO/IEC 27002** specification provides additional information on best practice and further guidance for implementation and maintenance of information security management system (ISMS). Controls listed in ISO 27001 Annex A are further explained in ISO 27002 document.

Mapping of MidPoint Features

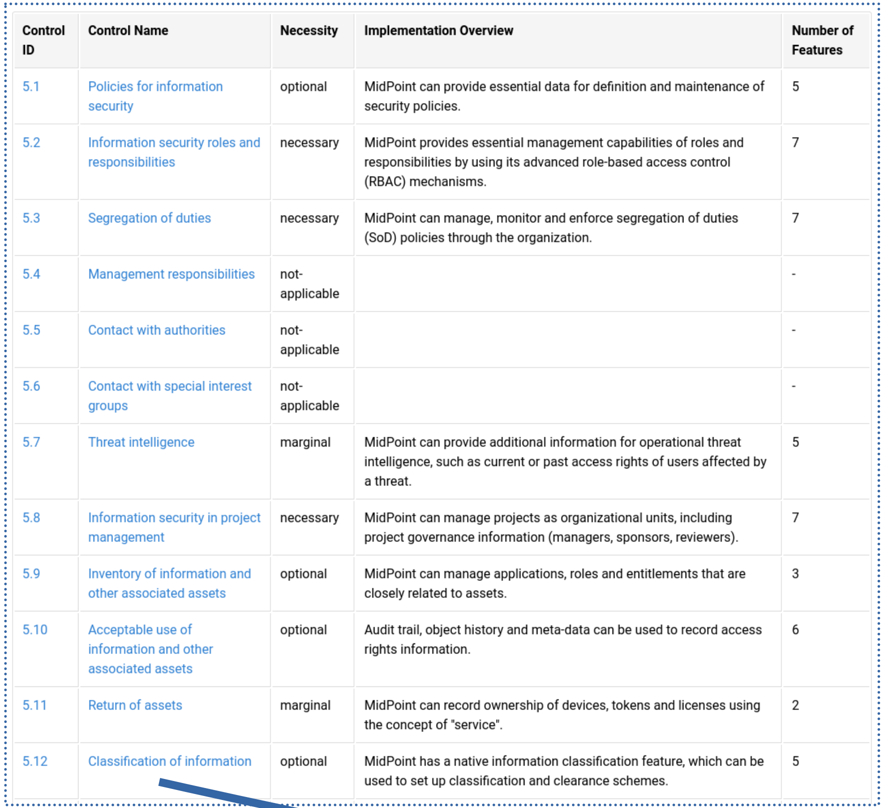
Control ID	Control Name	Necessity	Implementation Overview	Number of Features
5.1	Policies for information security	optional	MidPoint can provide essential data for definition and maintenance of security policies.	5
5.2	Information security roles and responsibilities	necessary	MidPoint provides essential 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

Documenting ISO/IEC 27001 Controls

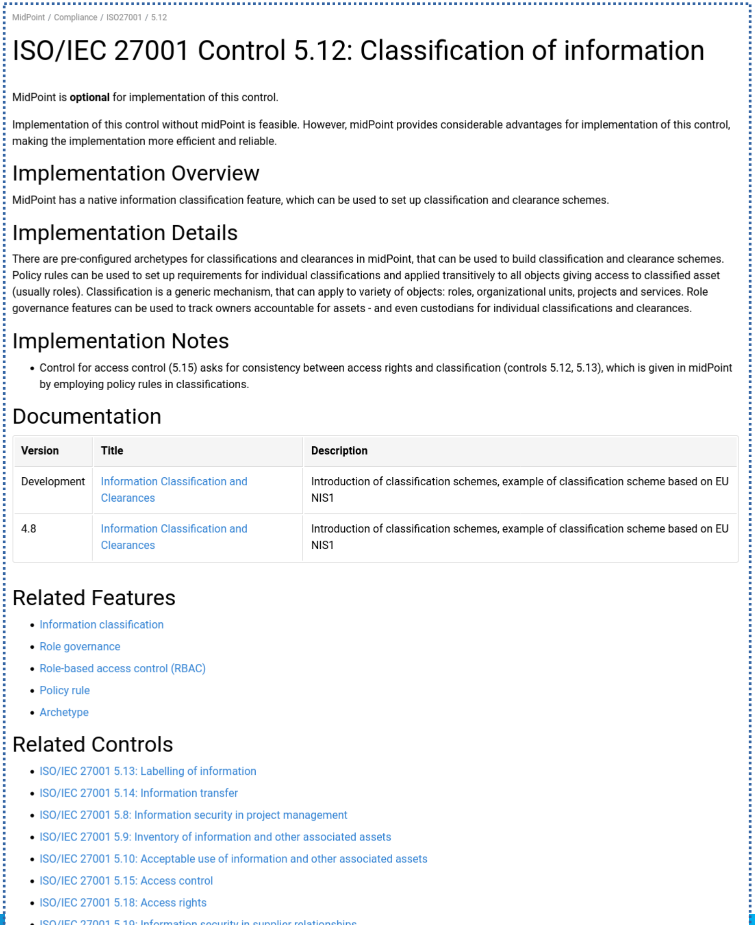
ISO 27000 and MidPoint

Work in progress

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

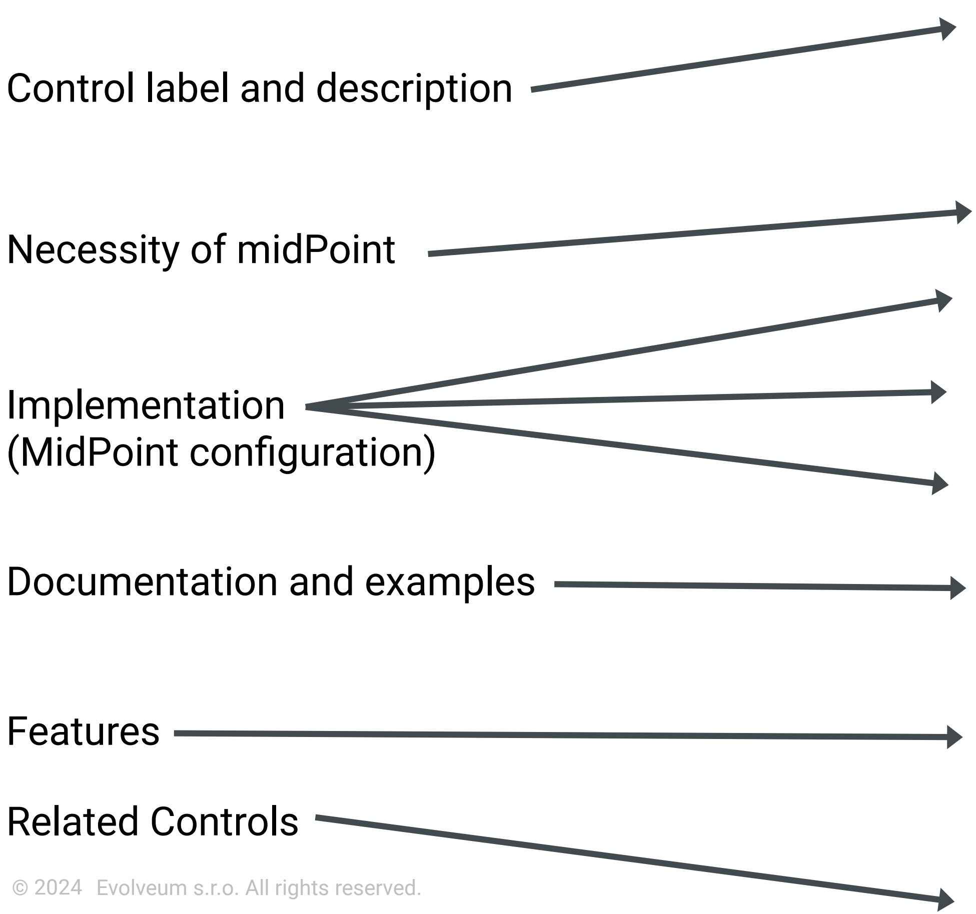
Related Controls

- 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

Documentation Example: Information Classification

ISO 27000 and MidPoint

Work in progress



Control label and description

Necessity of midPoint

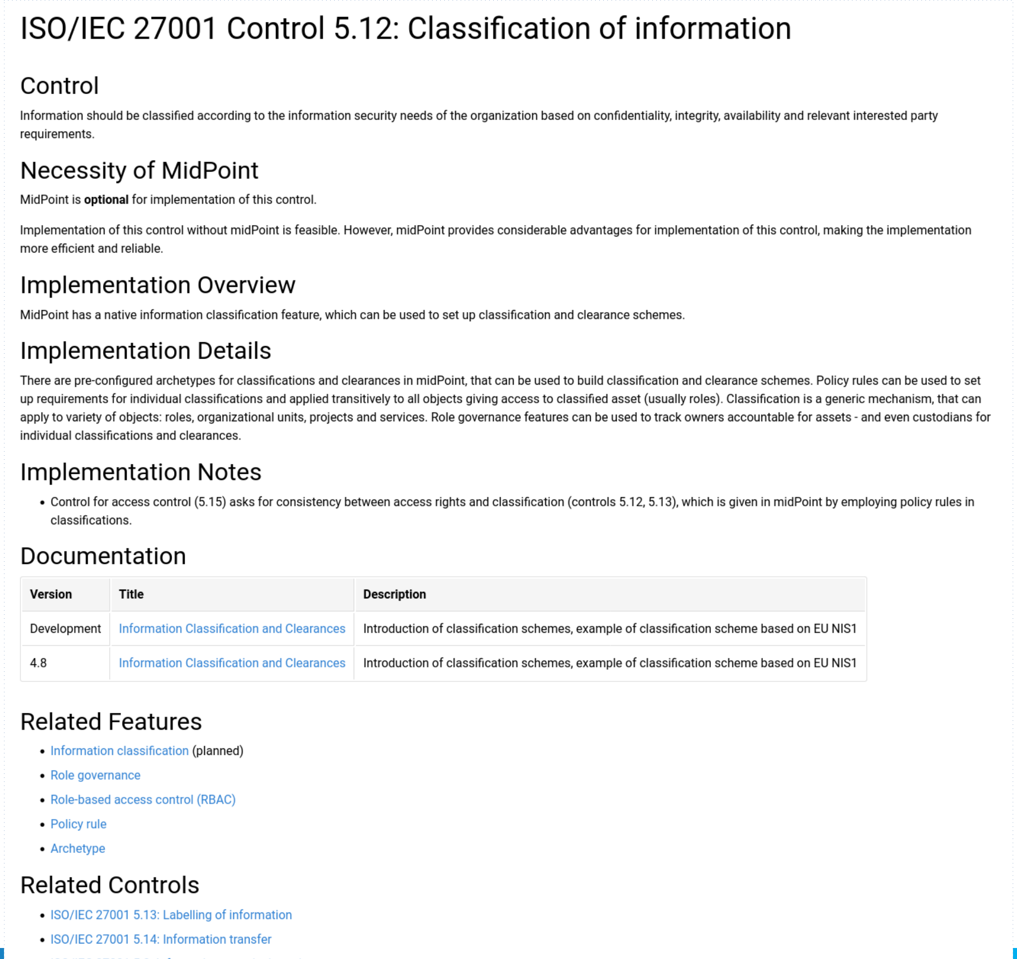
Implementation
(MidPoint configuration)

Documentation and examples

Features

Related Controls

https://docs.evolveum.com/midpoint/compliance/iso27001/5.12/



ISO/IEC 27001 Control 5.12: Classification of information

Control

Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.

Necessity of MidPoint

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

Related Controls

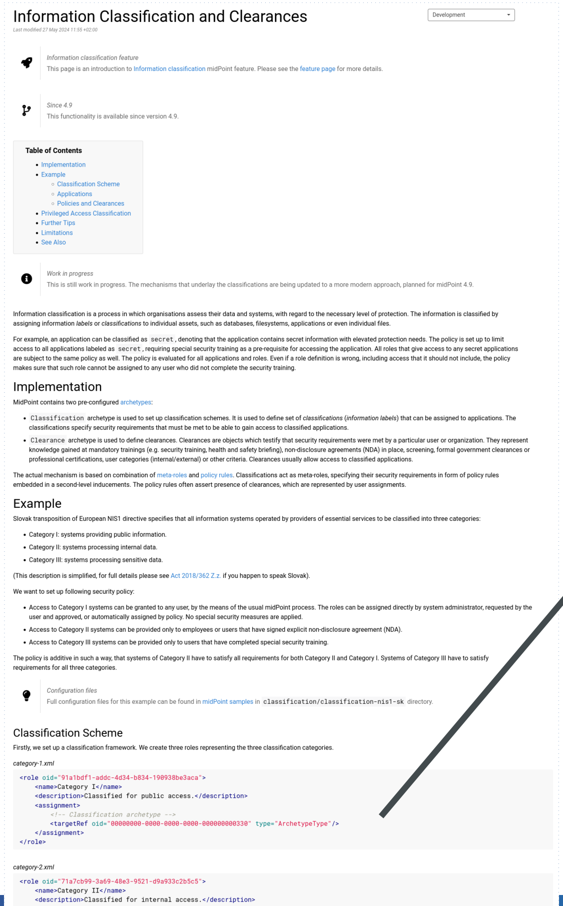
- ISO/IEC 27001 5.13: Labelling of information
- ISO/IEC 27001 5.14: Information transfer

Documentation Example: Information Classification

ISO 27000 and MidPoint

Work in progress

https://docs.evolveum.com/midpoint/reference/master/roles-policies/classification/



Information Classification and Clearances

Development

Last modified 27 May 2024 11:55 +02:00

Information classification feature

This page is an introduction to Information classification midPoint feature. Please see the feature page for more details.

Since 4.9

This functionality is available since version 4.9.

Table of Contents

- Implementation
- Example
  - Classification Scheme
  - Applications
  - Policies and Clearances
- Privileged Access Classification
- Further Tips
- Limitations
- See Also

Work in progress

This is still work in progress. The mechanisms that underlay the classifications are being updated to a more modern approach, planned for midPoint 4.9.

Information classification is a process in which organisations assess their data and systems, with regard to the necessary level of protection. The information is classified by assigning information *labels* or *classifications* to individual assets, such as databases, filesystems, applications or even individual files.

For example, an application can be classified as `secret`, denoting that the application contains secret information with elevated protection needs. The policy is set up to limit access to all applications labeled as `secret`, requiring special security training as a pre-requisite for accessing the application. All roles that give access to any secret applications are subject to the same policy as well. The policy is evaluated for all applications and roles. Even if a role definition is wrong, including access that it should not include, the policy makes sure that such role cannot be assigned to any user who did not complete the security training.

Implementation

MidPoint contains two pre-configured archetypes:

- `Classification` archetype is used to set up classification schemes. It is used to define set of *classifications* (*information labels*) that can be assigned to applications. The classifications specify security requirements that must be met to be able to gain access to classified applications.
- `Clearance` archetype is used to define clearances. Clearances are objects which testify that security requirements were met by a particular user or organization. They represent knowledge gained at mandatory trainings (e.g. security training, health and safety briefing), non-disclosure agreements (NDA) in place, screening, formal government clearances or professional certifications, user categories (internal/external) or other criteria. Clearances usually allow access to classified applications.

The actual mechanism is based on combination of meta-roles and policy rules. Classifications act as meta-roles, specifying their security requirements in form of policy rules embedded in a second-level inducements. The policy rules often assert presence of clearances, which are represented by user assignments.

Example

Slovak transposition of European NIS1 directive specifies that all information systems operated by providers of essential services to be classified into three categories:

- Category I: systems providing public information.
- Category II: systems processing internal data.
- Category III: systems processing sensitive data.

(This description is simplified, for full details please see Act 2018/362 Z.z. if you happen to speak Slovak).

We want to set up following security policy:

- Access to Category I systems can be granted to any user, by the means of the usual midPoint process. The roles can be assigned directly by system administrator, requested by the user and approved, or automatically assigned by policy. No special security measures are applied.
- Access to Category II systems can be provided only to employees or users that have signed explicit non-disclosure agreement (NDA).
- Access to Category III systems can be provided only to users that have completed special security training.

The policy is additive in such a way, that systems of Category II have to satisfy all requirements for both Category II and Category I. Systems of Category III have to satisfy requirements for all three categories.

Configuration files

Full configuration files for this example can be found in midPoint samples in `classification/classification-nis1-sk` directory.

Classification Scheme

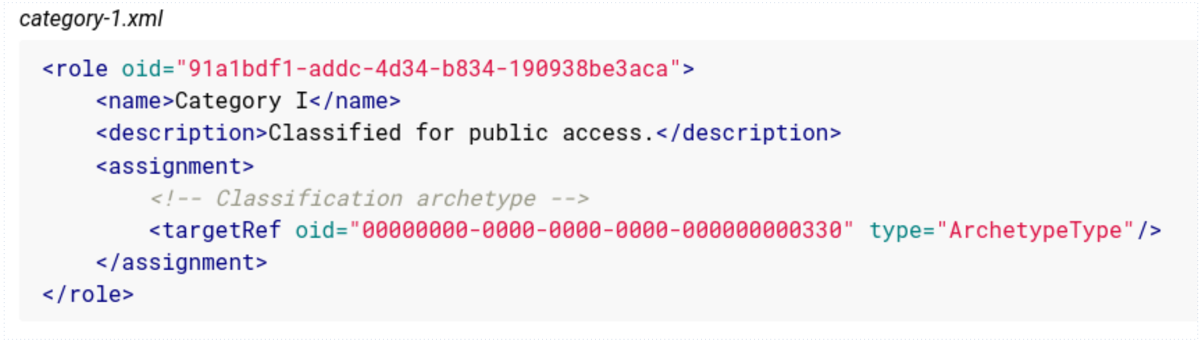
Firstly, we set up a classification framework. We create three roles representing the three classification categories.

category-1.xml

```
<role oid="91a1bdf1-addc-4d34-b834-190938be3aca">
    <name>Category I</name>
    <description>Classified for public access.</description>
    <assignment>
        <!-- Classification archetype -->
        <targetRef oid="00000000-0000-0000-0000-000000000330" type="ArchetypeType"/>
    </assignment>
</role>
```

category-2.xml

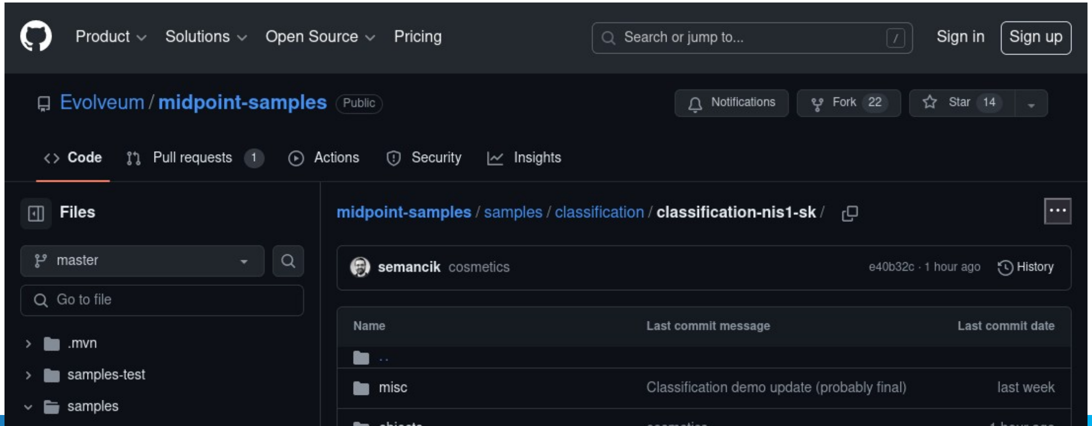
```
<role oid="71a7cb99-3a69-48e3-9521-d9a933c2b5c5">
    <name>Category II</name>
    <description>Classified for internal access.</description>
```



category-1.xml

```
<role oid="91a1bdf1-addc-4d34-b834-190938be3aca">
    <name>Category I</name>
    <description>Classified for public access.</description>
    <assignment>
        <!-- Classification archetype -->
        <targetRef oid="00000000-0000-0000-0000-000000000330" type="ArchetypeType"/>
    </assignment>
</role>
```

https://github.com/Evolveum/midpoint-samples/



- .mvn
- samples-test
- samples

midpoint-samples / samples / classification / classification-nis1-sk /

semancik cosmetics e40b32c · 1 hour ago History

Name	Last commit message	Last commit date
..		
misc	Classification demo update (probably final)	last week

Compliance Documentation: Plan

ISO 27000 and MidPoint

- Finish description of ISO 27001 controls (Summer 2024)
- Continually add new configuration examples (late 2024 and forever on)
- Work on other compliance frameworks, e.g. NIST CSF (2025)
- Evolveum compliance with ISO 27001 (late 2025)
- MidPoint features and improvements (4.9, 4.10, ...)

Disclaimer: This is a **plan**, it can change any time.

Approach to ISO/IEC 27001 Compliance

ISO 27000 and MidPoint

- MidPoint 4.8: baseline compliance
  - Features to address vast majority of ISO 27001 controls
  - Configuration may be less comfortable for advanced features
- MidPoint 4.9+: compliance improvements
  - New features aimed directly at compliance (ISO 27001, NIS 2, etc.)
  - Pre-configured for compliance
  - Easier and faster compliance
- Future: Built-in tooling for compliance
  - e.g. compliance checklists/dashboards

Compliance with MidPoint 4.9+

ISO 27000 and MidPoint

- **Certification improvements** [4.9]
- **Policy** as a first-class citizen (a.k.a. `PolicyType`) [4.9]
- Object **marks** for all objects (replacing `policySituation`) [4.9,4.10]
- Convenient management of **privileged access** [4.10]
- Convenient **GUI for policy rules** [4.10]
- **Outlier detection** and **role mining improvements** [4.9,4.10]
- Advanced **identity analytics** [4.10]

Disclaimer: This is a **plan**, it can change any time.

Demo

Information classification
midPoint 4.9 (development)

Demo Takeaways

ISO 27000 and MidPoint

- **Governance** is all about **high-level policies**
- **Governance policy rules** work **on top of** ordinary policies (e.g. RBAC)
- No user can violate* policy rules, not even superuser
- Policy rules can be used to **prove** that policies are maintained
- MidPoint can track **privileged access rights**
- **Information classification** is powerful and flexible mechanism

https://docs.evolveum.com/midpoint/reference/master/roles-policies/classification/
https://github.com/Evolveum/midpoint-samples/tree/master/samples/classification/classification-nis1-sk

* If they are set to enforcement. Of course, superuser can change them.

Conclusion

- **ISO/IEC 27000** is a series of **international standards** and **guidelines**
- It is related to other specifications **worldwide**
  - NIST CSF, NIS 2, DORA, GDPR, PSI DSS, HIPAA, ...
- ISO/IEC 27000 is quite specific and **technical**
- **IGA is necessary** for ISO/IEC 27001 compliance at scale
- **MidPoint** provides **numerous features**, even more to come
- Evolveum helps with **documentation** and **guidance**

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

Upcoming Webinars

- 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