MidPoint Community
Meetup 2025

Regulatory Compliance with MidPoint

Evolveum

Radovan Semančík, May 2025
Software Architect

Agenda

- Regulations
- Identity governance
- Policy rules for governance
- Demo

Regulations

International

- ISO 27001
- PCI-DSS

European

- NIS2
- DORA
- CSA
- CRA
- PLD
- CER
- AIA
- eIDAS 2.0
- GDPR
- ...

EU legislative hailstorm

USA

- NIST CSF
- SOC2
- NIST SP 800-53
- NIST SP 800-171
- HIPAA
- GLBA
- SOX
- ...

Regulations

International

- ISO 27001
- PCI-DSS

European

- NIS2
- DORA
- CSA
- CRA
- PLD
- CER
- AIA
- eIDAS 2.0
- GDPR
- ...

USA

- NIST CSF
- SOC2
- NIST SP 800-53
- NIST SP 800-171
- HIPAA
- GLBA
- SOX
- ...

ISO/IEC 27001:2022

Information security, cybersecurity and privacy protection
Information security management systems
Requirements

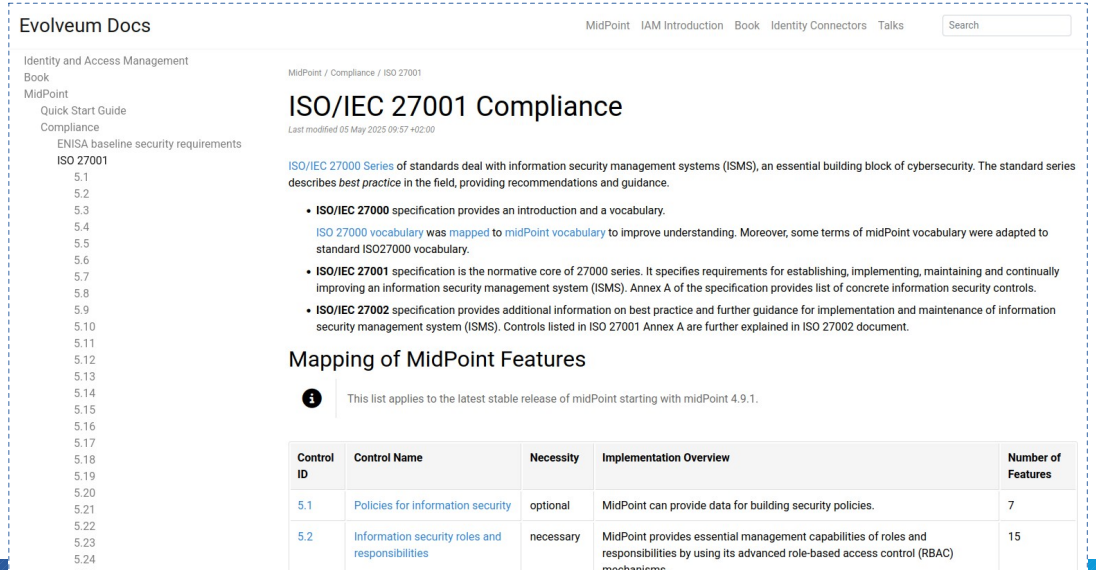
International Organization for Standardization (ISO)

- Technology standard
- Lists 93 concrete controls to be applied
- Risk-based
- Best practice (“voluntary” compliance)
- Referenced by other specs (NIS2, NIST CSF)

ISO/IEC 27001:2022

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
Quick Start Guide
Compliance
ENISA baseline security requirements
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

MidPoint / Compliance / ISO 27001

ISO/IEC 27001 Compliance

Last modified 05 May 2025 09:57 +02:00

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

This list applies to the latest stable release of midPoint starting with midPoint 4.9.1.

Control ID	Control Name	Necessity	Implementation Overview	Number of Features
5.1	Policies for information security	optional	MidPoint can provide data for building security policies.	7
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)	15

Evolveum

MidPoint Community Meetup 2025

ISO/IEC 27001:2022 Statement of Applicability (SoA)

	A	D	E	F
1	midPoint help			
2	midPoint Feature	Standard / Regulation / ...	Control	Occurence
3	Access certification	ISO27001	A.5.2, Information security roles and responsibilities, A.5.12, Classification and communication technology (ICT) supply-chain, A.5.22, Monitoring, rev	23
4	Access request process	ISO27001	A.5.12, Classification of information, A.5.15, Access control, A.5.16, Identit	8
5	Actions	ISO27001	A.5.24, Information security incident management planning and preparatio	2
6	Activation schema	ISO27001	A.5.16, Identity management, A.5.18, Access rights, A.5.19, Information se	19
7	Administration user interfac	ISO27001	A.8.15, Logging	1
8	Applicable policies	ISO27001	A.5.8, Information security in projectmanagement, A.5.15, Access control,	3
9	Application (concept)	ISO27001	A.5.15, Access control	1
10	Application inventory	ISO27001	A.5.1, Policies for information security, A.5.2, Information security roles and and communication technology (ICT) supply-chain, A.5.22, Monitoring, rev	28
11	Approval process	ISO27001	A.5.2, Information security roles and responsibilities, A.5.3, Segregation of	20
12	Archetype	ISO27001	A.5.8, Information security in projectmanagement, A.5.12, Classification of	12
13	Assignment	ISO27001	A.5.10, Acceptable use of information and other associated assets, A.5.12	19
14	Assignment metadata	ISO27001	A.5.10, Acceptable use of information and other associated assets, A.5.16	11
15	Asynchronous resources	ISO27001	A.5.16, Identity management	1
16	Attribute caching	ISO27001	A.8.14, Redundancy of information processing facilities	1
17	Audit trail	ISO27001	A.5.1, Policies for information security, A.5.10, Acceptable use of informati	39
18	Authorization	ISO27001	A.5.3, Segregation of duties, A.5.8, Information security in projectmanager	6
19	Auto-scaling	ISO27001	A.5.30, ICT readiness for business continuity, A.8.14, Redundancy of infor	2
20	Common identity managem	ISO27001	A.5.16, Identity management, A.5.34, Privacy and protection of personal id	4
21	ConnId identity connector fi	ISO27001	A.5.16, Identity management, A.5.23, Information security for use of cloud	9
22	Correlation	ISO27001	A.5.16, Identity management, A.8.32, Change management	2
23	Dashboard	ISO27001	A.5.1, Policies for information security, A.5.2, Information security roles and	22
24	Delegated administration	ISO27001	A.5.8, Information security in projectmanagement, A.5.15, Access control,	4
25	Documentation	ISO27001	A.5.16, Identity management, A.5.31, Legal, statutory, regulatory and contr	6
26	Entitlement	ISO27001	A.5.15, Access control, A.5.16, Identity management, A.5.18, Access right	16
27	Entitlement association	ISO27001	A.5.15, Access control, A.5.16, Identity management, A.5.18, Access right	16
28	Escalation	ISO27001	A.5.2, Information security roles and responsibilities	1
29	Expression	ISO27001	A.5.16, Identity management, A.8.11, Data masking	2
30	Flexible authentication	ISO27001	A.5.17, Authentication information, A.8.3, Information access restriction, A.	3

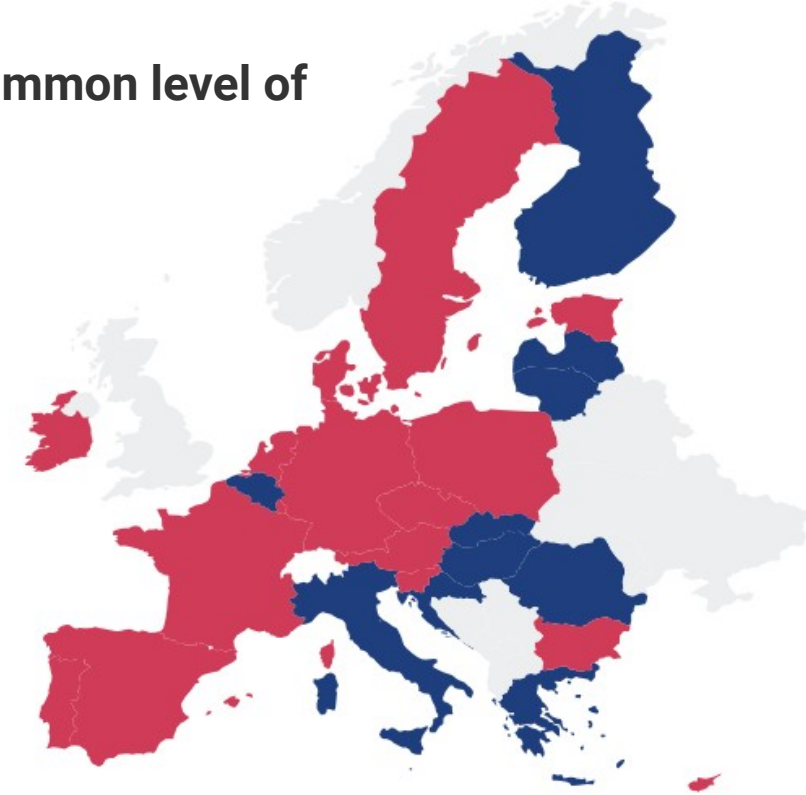
Evolveum

MidPoint Community Meetup 2025

NIS2

Directive (EU) 2022/2555 ... on measures for a high common level of cybersecurity across the Union, …

European Parliament and the Council (EU)



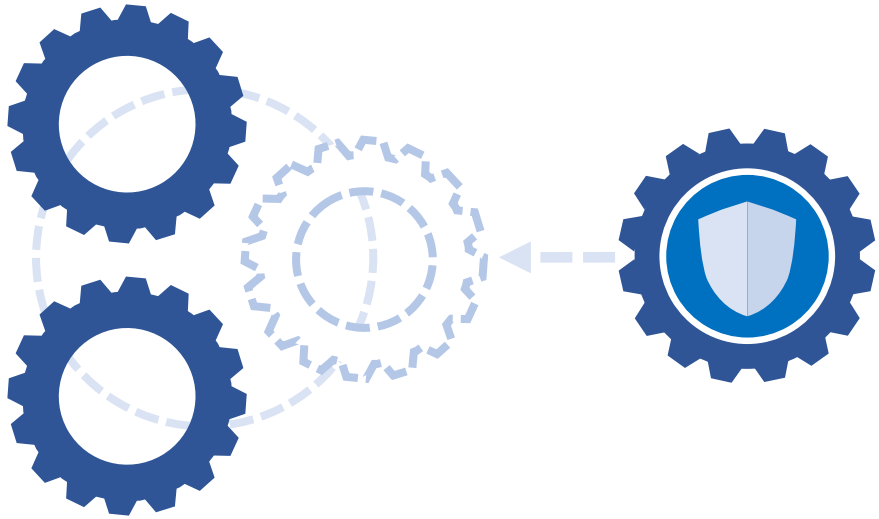
https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

- EU legislation (to be applied by 18th October 2024)
- High-level requirements (not very technical)
- Directive → slow adoption
- Variations in local legislation

Regulatory Compliance & midPoint

- Identity governance: superpower of midPoint
- Pre-configured for compliance (in progress)

  policy rules, reports, dashboard, ...
- Documentation



Identity Governance

- Access control governance: *Why does user have access?*

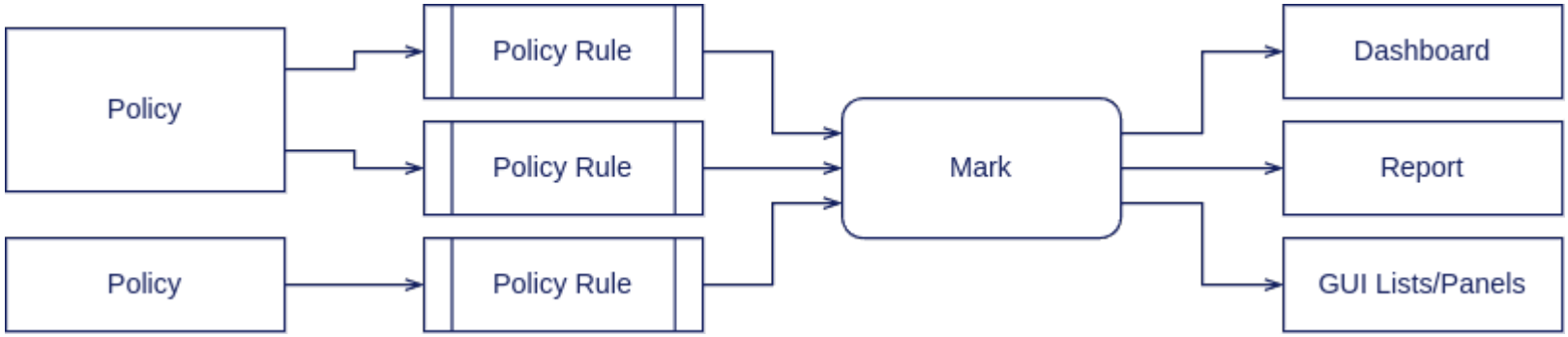
  reports, reviews, meta-data, ...

- Responsibility: *Who is responsible for what?*

  owners, approvers, teams, roles, ...

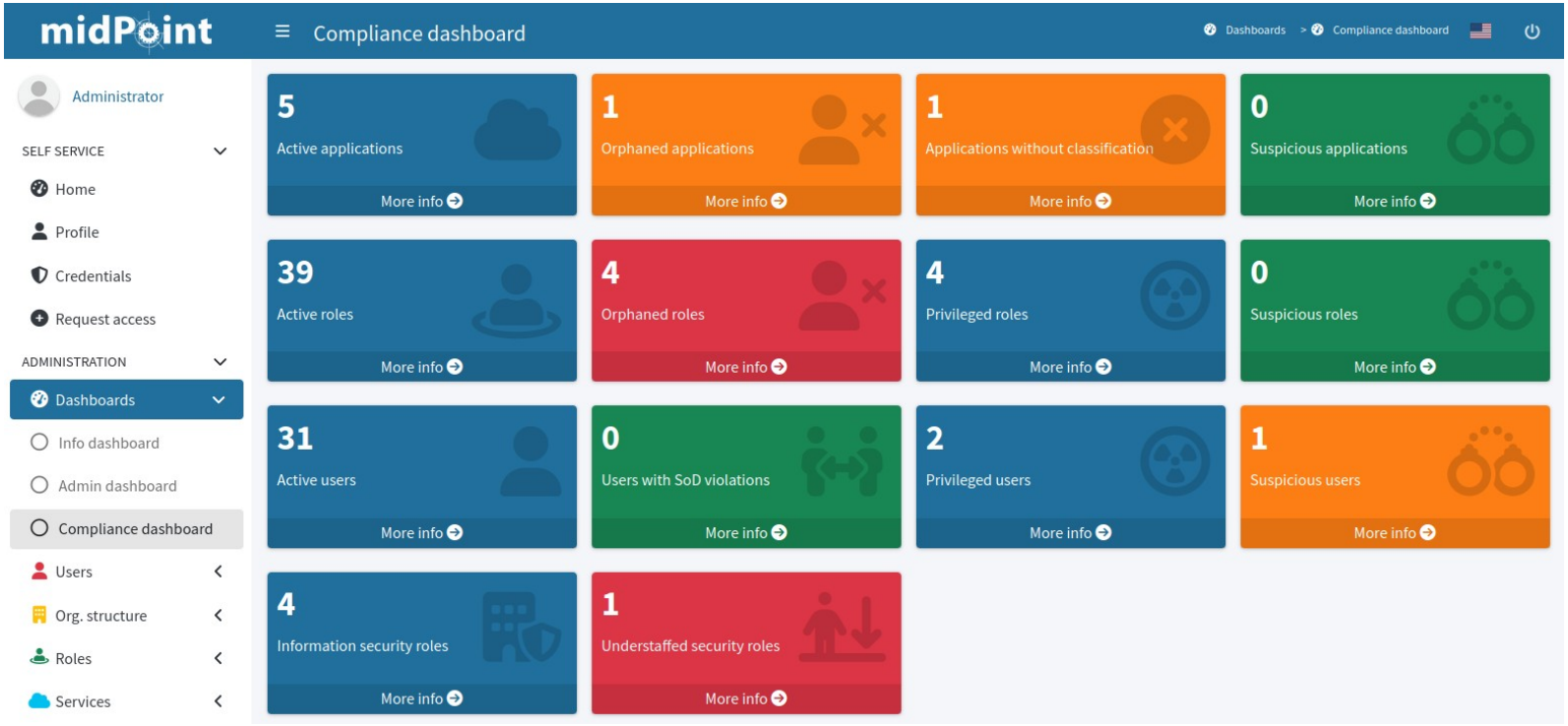
- High-level policies (business oriented)
- Make sure we data and policies properly managed

Policy Rules for Governance



- Applications/roles without owners (“orphaned”)
- Understaffed roles/orgs
- Privileged roles/users
- Unclassified applications
- Suspicious objects (manual mark)

Compliance Dashboard



Color code: blue = info, green = compliant, orange = warning, red = non-compliant

DEMO

Compliance Policy Rules

midPoint 4.10 (development)

Configuration:

https://github.com/Evolveum/midpoint-samples/tree/master/samples/compliance

© 2025 Evolveum s.r.o. All rights reserved.

Evolveum

Conclusion

- Cybersecurity regulations are widespread
- Identity governance is a crucial part of regulatory compliance
- MidPoint can help
- Ambition: make compliance easier out-of-the-box

Evolveum

Thank you for your attention

Feel free to ask your questions now!

MidPoint Community Meetup 2025