MidPoint Working Group at TIIME 2024

MidPoint and Cybersecurity Compliance

Radovan Semančík
Evolveum's Co-Founder and Software Architect

Agenda

- Cybersecurity and compliance
- Regulations and Standards
- How can we help?
- ISO27001 (preview)
- Plans
- Discussion

Introduction

- Cybersecurity crisis
- Poor practice → low security → breaches
- Visibility problem
- Countries react by cybersecurity regulations
- **Compliance** with cybersecurity regulations and best practice

Regulations and Standards

- **ISO27001:2002**
- **NIS2**
- **NIST CSF**
- GDPR
- PCI DSS
- HIPAA
- SOX
- COBIT 2019
- ...

ISO27001:2022

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)

NIS2

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

European Parliament and the Council (EU)

- EU legislation (to be applied by 18th October 2024)
- High-level requirements (not very technical)
- Alignment of legislation across EU member states
- Stricter requirements than NIS1: broader scope, fines, personal responsibility

NIS2 and MidPoint

- NIS2 encourages the use of innovative technology, incl. AI (Part1-15)
- NIS2 encourages the use of open source (Part1-52)
- NIS2 explicitly mentions IAM (Part1-89)
- NIS2 reporting obligations
  would be almost impossible to satisfy without IGA
- NIS2 points to “state-of-the-art” and “industry best practice”
  → ISO27001, NIST CSF

NIST Cybersecurity Framework

Framework for Improving Critical Infrastructure Cybersecurity

U.S. National Institute of Standards and Technology (NIST)

- Version 2.0: final draft in early 2024 (NIST CSWP 29)
- Guidelines, mandatory for U.S. federal agencies and their contractors
- Used internationally as general best practice
- Risk-based

How Can We Help?

- IGA is absolutely essential component of cybersecurity
- No direct out-of-the-box compliance
  - midPoint cannot be “ISO27001 certified”
- However, we **can** help customers with compliance
  - Statement of Applicability (SoA)
  - Recommendations for midPoint configuration
  - Documentation
  - Future: Built-in tooling (e.g. compliance checklists/dashboards)
- Starting with ISO27001:2022

Preview: ISO27001 Statement of Applicability (Summary)

Work in progress: preliminary results

Category	Number of controls	midPoint coverage	Percentage
Organizational	37	26	70 %
People	8	7	88 %
Physical	14	2	14 %
Technological	34	22	65 %
Total	**93**	**57**	**61 %**

14 controls are almost impossible to implement without IGA platform in place

Preview: ISO27001 Statement of Applicability (Spreadsheet)

Work in progress: preliminary results

ISO/IEC 27001:2022 Statement of Applicab				
Sectio	Contr	Control	Control applicable ?	Reference to Control Document/Evidence
A5 - Orga	A.5.1	Policies for information security	0	midPoint segregation of duties
A5 - Orga	A.5.2	Information security roles and responsibilities	1	midPoint segregation of duties
A5 - Orga	A.5.3	Segregation of duties	1	segregation of duties
A5 - Orga	A.5.4	Management responsibilities	0	
A5 - Orga	A.5.5	Contact with authorities	0	
A5 - Orga	A.5.6	Contact with special interest groups	0	midPoint segregation of duties

Preview: ISO27001 Statement of Applicability (Text)

Work in progress: preliminary results

5.18 Access rights

Role of midPoint: **necessary**

midPoint offers possibilities for creating business access roles that are easier managed. Customers can define approval procedures for granting access rights. Roles can be tagged for segregation of duties with selected behavior (e.g., automatic rejection). All the changes are recorded and available via logs also many changes and settings can be inspected directly in midPoint. Since midPoint can aggregate user identities from a lot of different systems, it can serve as a central point for access rights to all of the systems. With a recertification campaign it is possible to regularly check and control if access rights are still valid and proper. Important feature for all access roles is the possibility to set time expiration of access rights.

5.19 Information security in supplier relationships

Role of midPoint: **optional**

midPoint can manage access rights of suppliers, e.g., by creating temporary access rights automatically revoked on expired date, by creating a business role especially created for a specific supplier that can be easily monitored (who has access to that role) and revoked.

MidPoint ISO27001 Statement of Applicability (SoA)

- Starting point for midPoint evaluation and deployment
- Needs to be customized for ISO compliance, reflecting real configuration and processes
- Still work in progress

Documentation Links

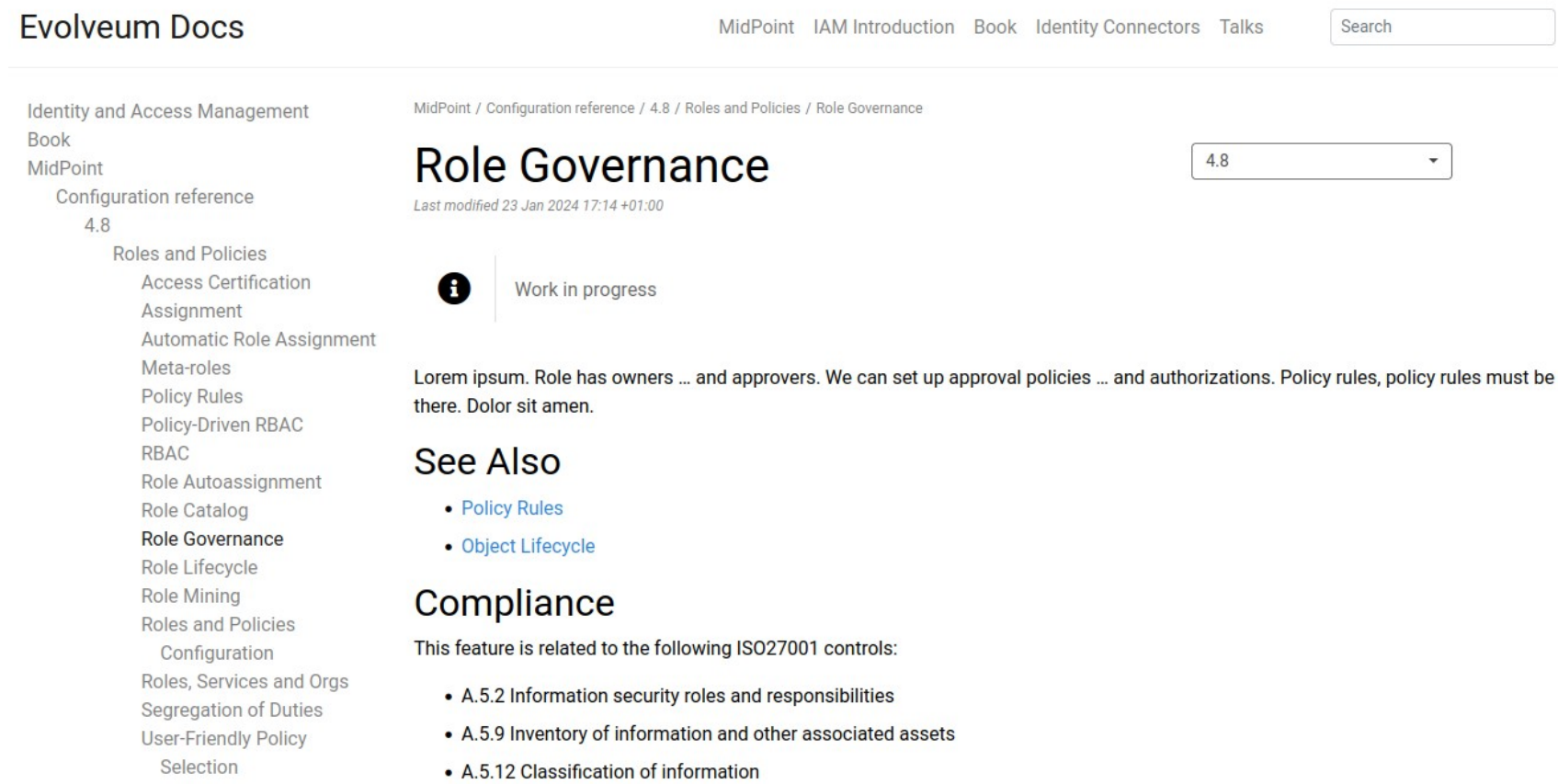
MidPoint / Compliance / ISO27001

ISO27001 Compliance

Last modified 24 Jan 2024 13:22 +01:00

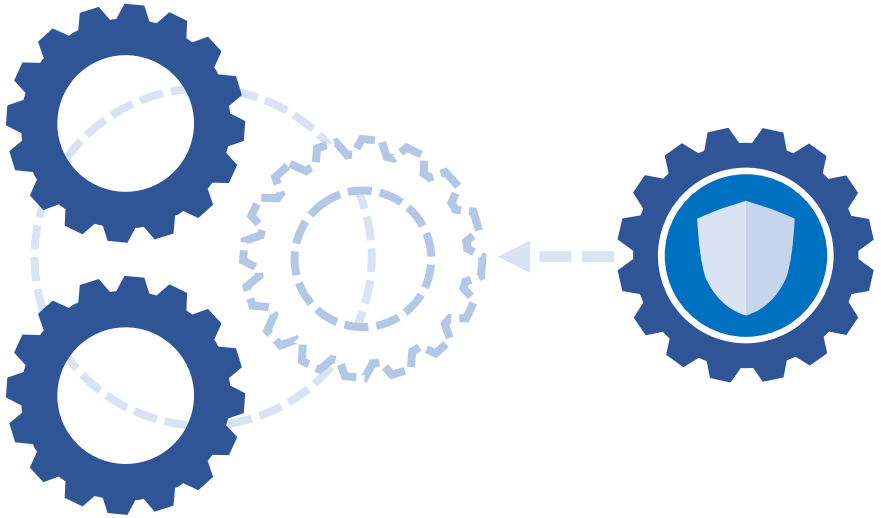
Control ID	Control Name	Necessity	Features
A.5.2	Information security roles and responsibilities	optional	Role governance Approval process Delegated administration
A.5.3	Segregation of duties	necessary	Segregation of duties
A.5.9	Inventory of information and other associated assets	optional	Role governance Application inventory
A.5.10	Acceptable use of information and other associated assets	necessary	Object lifecycle Object metadata Access certification Micro-certification
A.5.12	Classification of information	optional	Role governance

Documentation Links



Plans

- Finish ISO27001 Statement of Applicability
- Documentation links and improvements
- Configuration suggestions
- NIS2 Statement of Applicability (as much as possible)
- NIST CSF?








Discussion

Do you know where to start with cybersecurity compliance?
Experiences/expectations with NIS1/NIS2?
Which regulations/standards are necessary for you?
Any missing features?
Are you using midPoint for compliance already? Experiences?

Conclusion

- **Compliance** with cybersecurity regulations and best practice
- ISO27001, NIS2, NIST CSF, ...
- It is **necessary**, for the benefit of us all
- It will be slow, painful and never-ending process
- **MidPoint can help**, make it faster and less painful
- We are working on it


Thank you for your attention
Feel free to ask your questions now!
TIIME
MidPoint Working Group at TIIME 2024