Regulatory Compliance with MidPoint

Radovan Semančík, June 2025
Software Architect

Agenda

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

Evolveum

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
- ...

Evolveum

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
- ...

Evolveum

ISO/IEC 27001:2022

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

International Organization for Standardization (ISO)

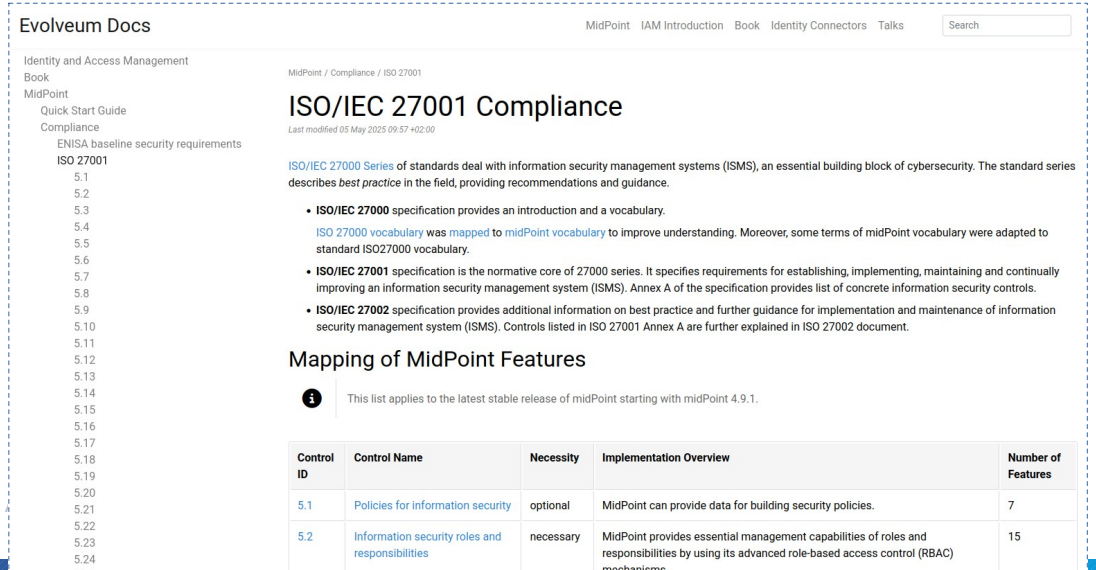
- Technology standard
- Lists 93 concrete controls to be applied
- Risk-based
- Best practice (“voluntary” compliance)
- Referenced by other specs (NIS2, NIST CSF)

Evolveum

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) mechanisms.	15

Evolveum

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

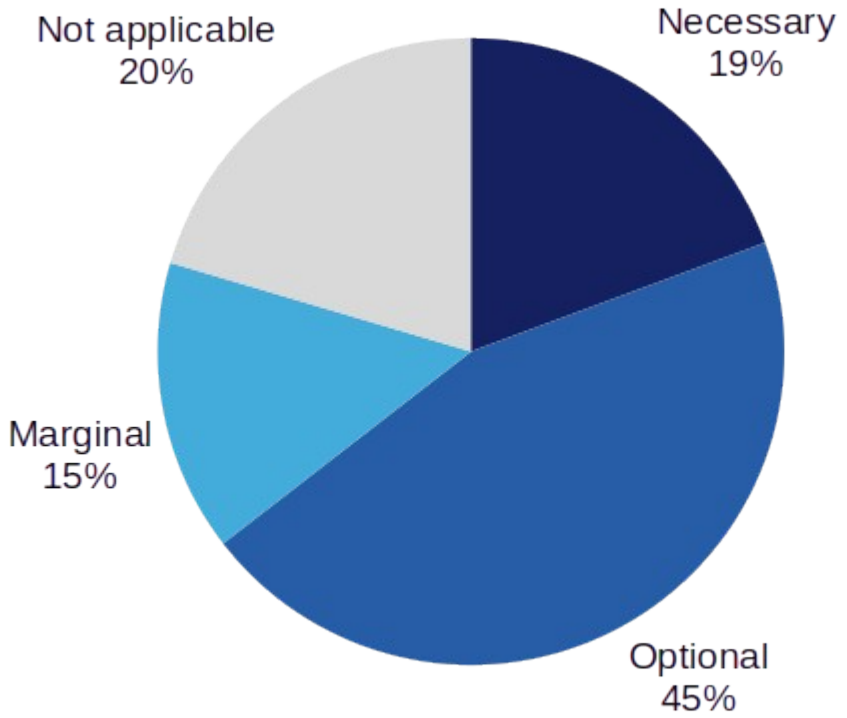
https://docs.evolveum.com/midpoint/compliance/iso27001/soa/

	A	B	C	D	J	K
1	ISO/IEC 27001:2022 Statement of Applicability					
2	Section	Contro	Control	Control Description	Control applicable?	midPoint features
3	A5 - Organization control	A.5.1	Policies for information security	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Optional	Reporting Simulation Audit trail Application inventory Dashboard Policy rule Object mark
4	A5 - Organization control	A.5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Necessary	Role-based access control (RBAC) Role catalog Object governance Information classification (planned) Simulation Application inventory Relation Organizational structure Access certification Escalation Policy rule Policy (concept) (planned) Approval process Reporting Dashboard
5	A5 - Organization control	A.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	Necessary	Segregation of duties (SoD) Policy rule Meta-role Gradual policy enforcement Approval process Authorization Reporting
6	A5 - Organization control	A.5.4	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Not applicable	

Evolveum

ISO/IEC 27001:2022 Controls Supported By MidPoint

	Controls	
Necessary	18	19%
Optional	42	45%
Marginal	14	15%
Not applicable	19	20%
Total	93	

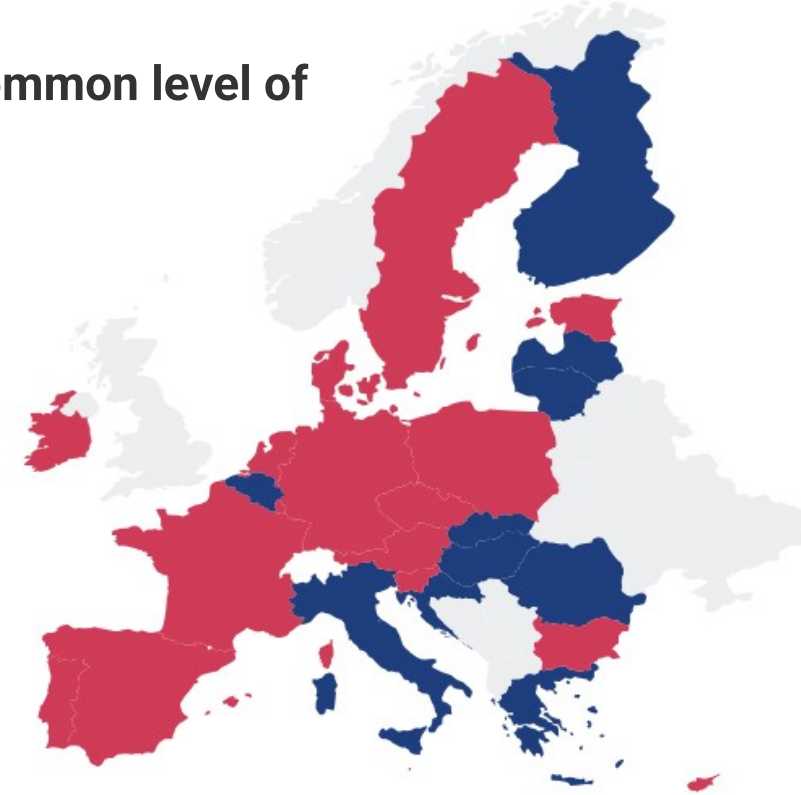


Evolveum

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/

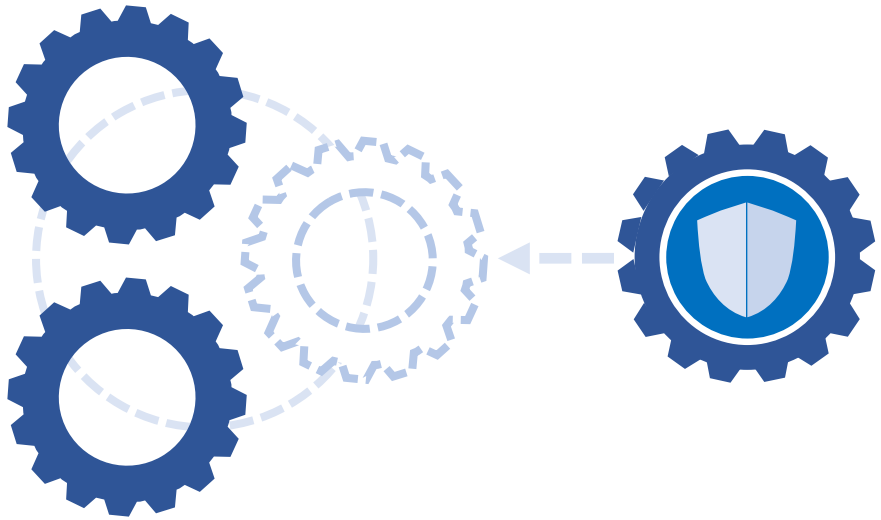
- EU legislation (to be applied by 18th October 2024)
- High-level requirements (not very technical)
- Directive → inconsistent and slow adoption
- Variations in local legislation

Evolveum

Regulatory Compliance & MidPoint

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

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



Evolveum

Identity Governance

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

  reports, reviews, meta-data, ...

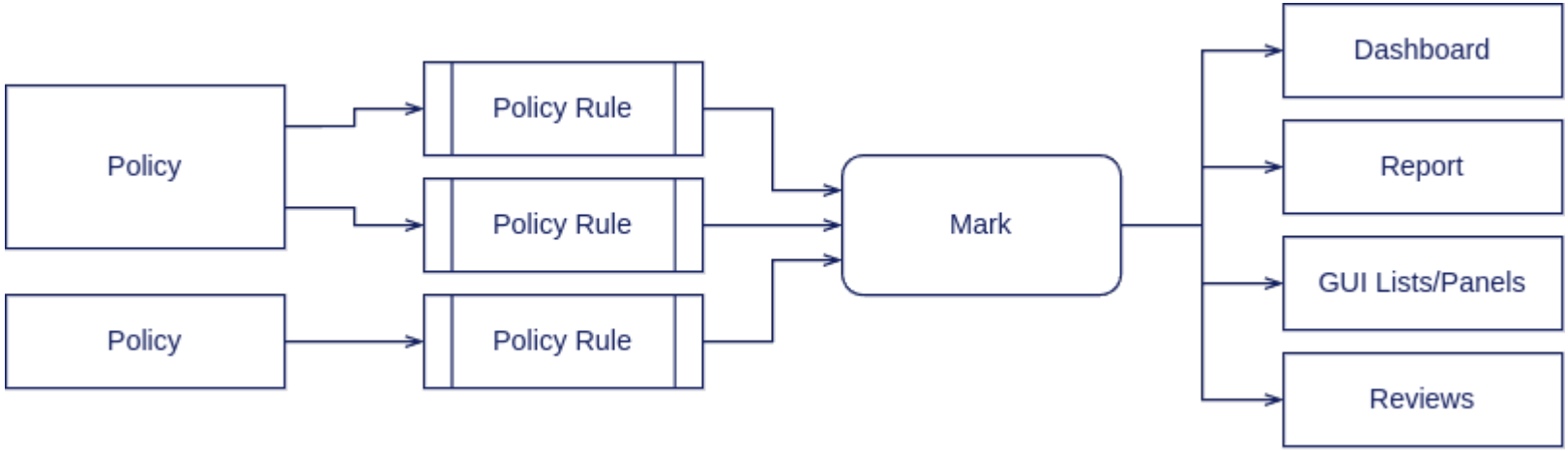
- Responsibility: *Who is* ***responsible*** *for what?*

  owners, approvers, teams, roles, ...

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

Evolveum

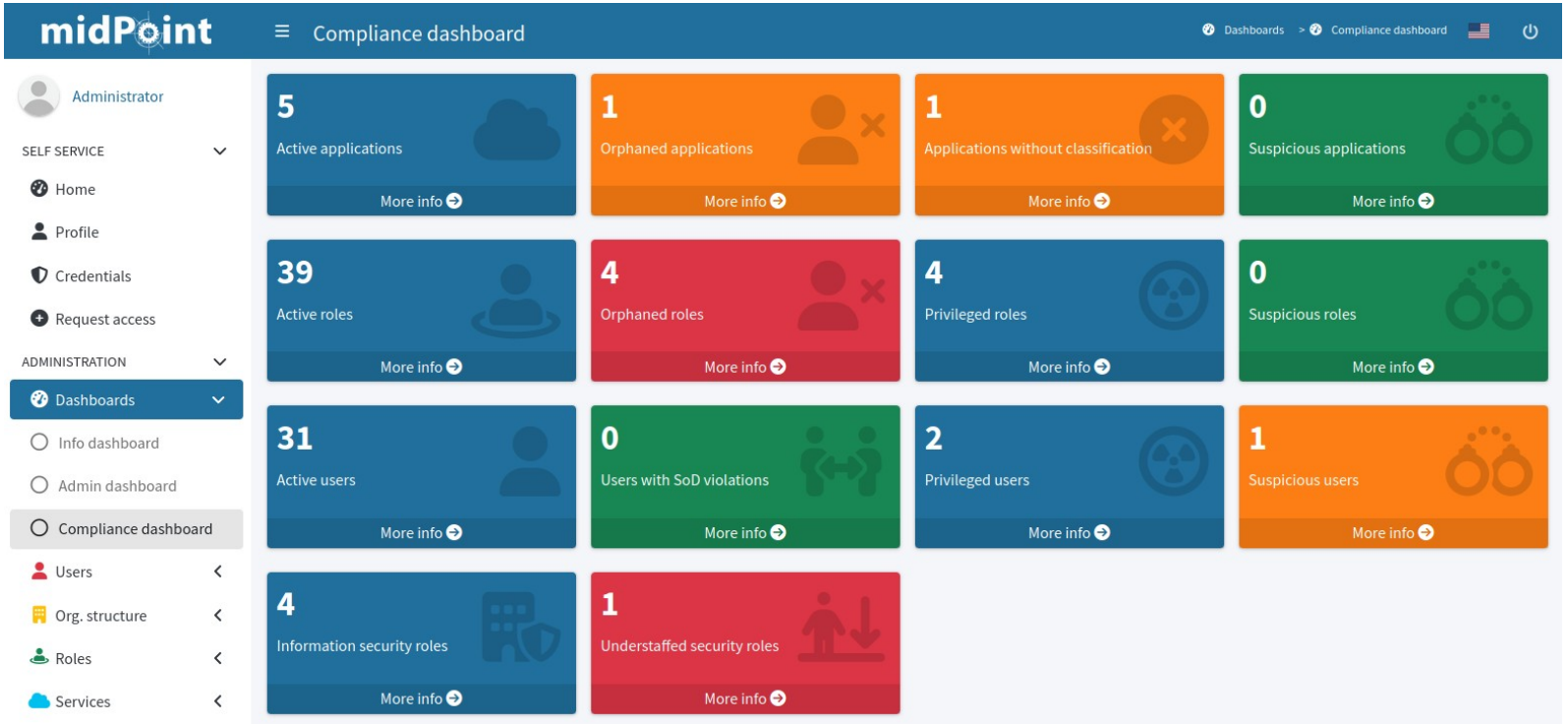
Policy Rules for Governance



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

Evolveum

Compliance Dashboard



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

Evolveum

Demo: Compliance Policy Rules

Enforcing high-level identity governance rules:

- Every application should have an owner
- Every application should have a classification
- Every business role should have an owner
- Mark application roles granting privileged access
- Track users that have privileged access

Evolveum

DEMO

Compliance Policy Rules

midPoint 4.10 (development)

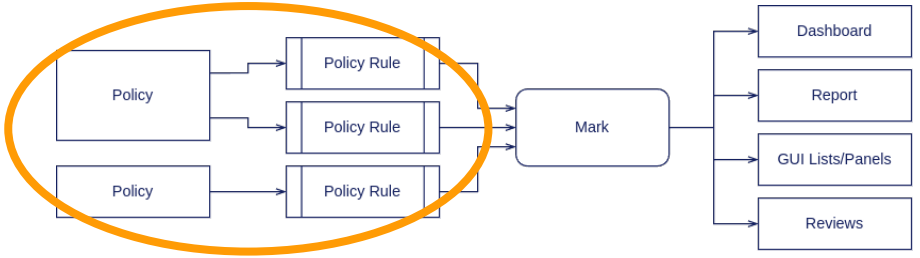
Configuration:

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

Documentation:

https://docs.evolveum.com/midpoint/reference/master/roles-policies/identity-governance-rules/

Configuration: Enforcing Application Owners

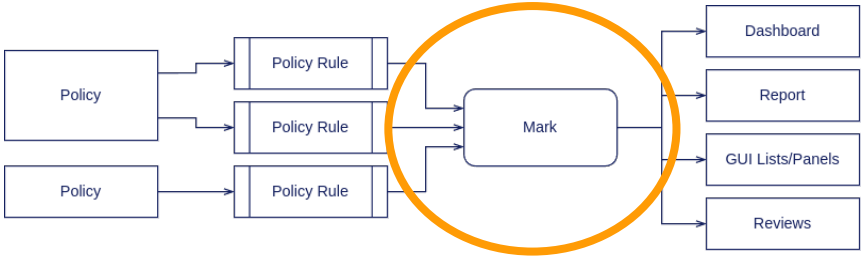



```
<archetype oid="00000000-0000-0000-0000-000000000329">
    <name>Application</name>
    ...
    <inducement>
        <policyRule>
            <policyConstraints>
                <minAssignees>
                    <multiplicity>1</multiplicity>
                    <relation>org:owner</relation>
                </minAssignees>
            </policyConstraints>
            <markRef oid="5508aca4-2aef-47a6-ad50-892389823c91"/> <!-- "Orphaned" mark -->
            <policyActions>
                <record/>
            </policyActions>
            <evaluationTarget>object</evaluationTarget>
        </policyRule>
    </inducement>
</archetype>
```


https://docs.evolveum.com/midpoint/reference/master/roles-policies/identity-governance-rules/

Evolveum

Configuration: Enforcing Application Owners

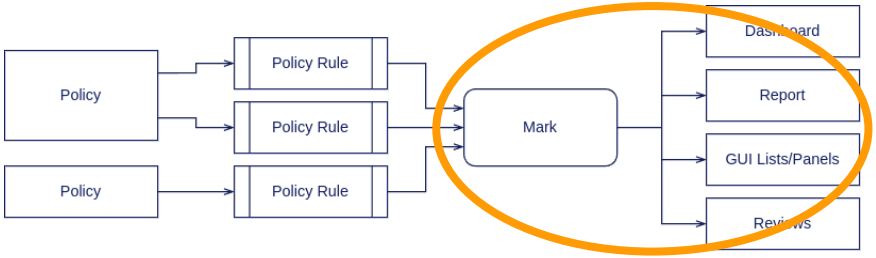



```
<mark oid="5508aca4-2aef-47a6-ad50-892389823c91">
    <name>Orphaned</name>
    <description>Mark for object which does not have an owner.</description>
    <display>
        <icon>
            <cssClass>fa fa-user-xmark</cssClass>
        </icon>
    </display>
    <assignment id="1">
        <identifier>archetype</identifier>
        <targetRef oid="00000000-0000-0000-0000-000000000701" type="ArchetypeType"/>
    </assignment>
</mark>
```


https://docs.evolveum.com/midpoint/reference/master/roles-policies/identity-governance-rules/

Evolveum

Configuration: Enforcing Application Owners

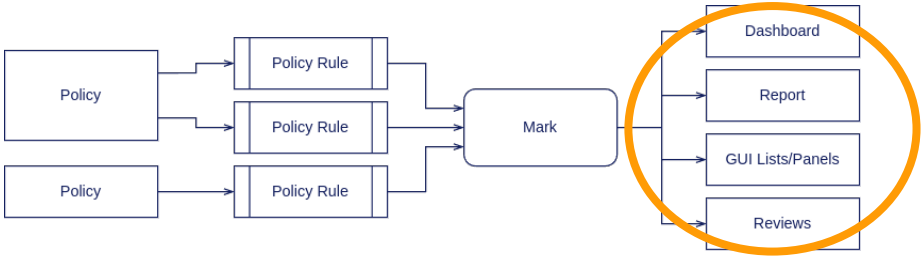



```
<mark oid="5508aca4-2aef-47a6-ad50-892389823c91">
    <name>Orphaned</name>
    <description>Mark for object which does not have an owner.</description>
    <display>
        <icon>
            <cssClass>fa fa-user-xmark</cssClass>
        </icon>
    </display>
    <assignment id="1">
        <identifier>archetype</identifier>
        <targetRef oid="00000000-0000-0000-0000-000000000701" type="ArchetypeType"/>
    </assignment>
</mark>
```

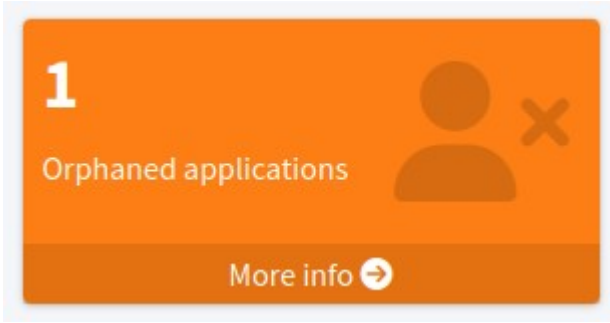
effectiveMarkRef matches (oid = "5508aca4-2aef-47a6-ad50-892389823c91")

https://docs.evolveum.com/midpoint/reference/master/roles-policies/identity-governance-rules/

Configuration: Enforcing Application Owners

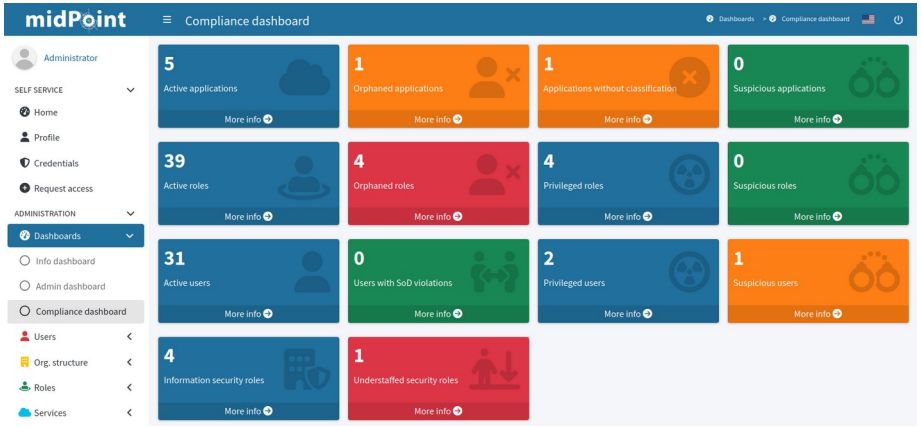



```
<dashboard oid="f941f3fc-dcef-4415-9e79-ae56b185a501">
    ....
    <widget>
        ...
        <data>
            <sourceType>objectCollection</sourceType>
            <collection>
                <collectionRef oid="cc8c1397-e5c4-456c-bd98-f07b3dca97ec" type="ObjectCollectionType"/>
            </collection>
        </data>
        <presentation>
            <dataField>
                <fieldType>value</fieldType>
                <expression>
                    <proportional>
                        <style>value-only</style>
                    </proportional>
                </expression>
            </dataField>
        </presentation>
    </widget>
</dashboard>
```



https://docs.evolveum.com/midpoint/reference/master/roles-policies/identity-governance-rules/

Demo Summary



- Demo: Compliance Policy Rules
- Works on midPoint 4.10 (development)
- Configuration:
  MidPoint Studio project, see README
  https://github.com/Evolveum/midpoint-samples/tree/master/samples/compliance
- Documentation (partial):
  https://docs.evolveum.com/midpoint/reference/master/roles-policies/identity-governance-rules/
- Part of the configuration will be provided out-of-the-box (initial objects) in midPoint 4.10

Evolveum

Cybersecurity Made In Europe

- Founded by European Cyber Security Organisation (ECSO)
- European companies (ownership and R&D)
- Cybersecurity requirements (ENISA)

- Our commitment to EU legislation compliance (e.g. Cyber Resilience Act, AI Act, GDPR, ...)
- European digital sovereignty

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
- EU legislation compliance and digital sovereignty

Evolveum

Questions & Answers

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

Funded by the European Union
NextGenerationEU
RECOVERY AND RESILIENCE PLAN

Evolveum