SIG-ISM
ISO work @ SUNET

David Heed, Coordinator Sunet security center
GN5-1 WP8 T3 co-tasklead

Agenda

- Intro
- Previous work
- Current work
  - What can be automated
  - “Year wheel”
- Standards

Background

Local legislation

External legal requirements

More audits

Oncoming legislation (NIS2 etc)

Inventory and Pre-work

- Identify all relevant services and their dependencies.
- Define key processes related to the services.
- Determine which data needs to be included in the shared inventory to facilitate audit and certification processes.
- Specify the components included in each service and their respective configurations.
- Create and maintain documentation of the inventory and link it to existing policies. Ensure a comprehensive index of supporting documents is created and accessible.

Definitions and common work items

Work on regulations to technical format

- Can we perform technical and automated checks for verification of compliance?

Develop routines and procedures for how should tags and code repositories be handled

Perform dry-runs and automated audits on federation services SWAMID and eduGain

Verification of inventory and dataset consistency

Administrative work

Getting grouplicense för ISO27001 and adjacent standards

Case studies with other companies automating or supporting automation.

Evaluate GRC tooling

Vetenskapsrådet

Automating security checks

OSCAL (Open Security Controls Assessment Language)

- Machine readable security control definitions
- Automated Validation of controls Mapping / scale for all services
- Streamline continuous monitoring / scale for all services
- Facilitate audit documentation
- Integrate with GRC tools

Year wheel - repeating activities

- Risk Analysis
- Risk Management Plan
- Review of Asset Register
- Update Information Security Policy
- Approve Updated Policy
- Update Guidelines
- Approve Updated Guidelines
- Security Awareness Training
- Management Review
- Internal Audit
- Access Inventory
- Physical Security Control
- Review Continuity Plans
- Test Continuity Plans
- Review/Audit Suppliers
- Independent Policy Review

ISO/IEC standards we put in scope

- ISO/IEC 27001:2022 — Information security, cybersecurity, and privacy protection – Requirements for information security management systems.
- ISO/IEC 27002:2022 — Information security controls for cybersecurity and privacy protection.
- ISO/IEC 27005:2022 — Guidelines for managing information security risks.
- ISO/IEC 27701:2019 — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management systems – Requirements and guidelines.

Collaborate?

Want to have a working group on automating security audits and GRC work?

We have an ongoing internal project and welcome discussions on joint engineering or just documenting common requirements for deciding on tools and way forward.

Any others done evaluation on automation for GRC tooling?