SIG-ISM Meeting Fall 2025

10th anniversary meeting of SIG-ISM, RedIRIS, Madrid, Spain

07./08.10.2025

Introductions

- Let‘s see who is participating

Welcome to RedIRIS

Connecting universities and Spanish R&D&I since 1988

www.rediris.es

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
RedIRIS

Social Activity – Guided Tour

The touristic visit will start at 19:00

Meeting point

Statue of King Charles III, Puerta del Sol, Madrid.

Social dinner

Dinner:

Restaurant Name: El Imparcial

Address: Duque de Alba 4, https://maps.app.goo.gl/fR6WewcTG3jZwKcN7

Agenda

Tuesday 7th

13-15 Session 1

- the past, the now and the future
- What is GÉANT doing

15-15:15 Coffee break

15:15-17 Session 2

- Compliance panel
- Open table discussions

19:00 Sightseeing tour, Puerta del Sol

20:30 dinner at El Imparcial

Wednesday 8th

09:30-11 Session 3

- Communication
- A.I. and Security panel

11-11:15 Coffee break

11:15-13 Session 4

- Vulnerability lookup tool (CIRCL)
- Time to share and present
- Open table discussions

13-14 lunch and goodbye

The past: 10 years of SIG-ISM

- Presentation by long time SC members Alf, Rolf & Urpo

The now

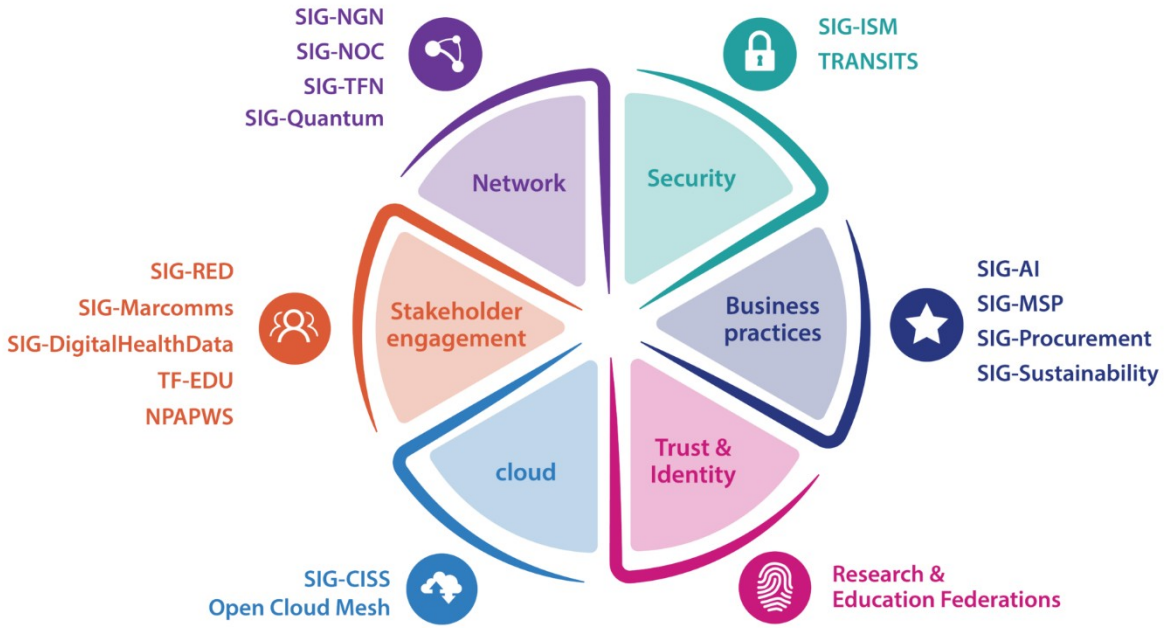
- New steering committee members since Winter 2024
  - Cynthia Wagner, RESTENA
  - Kathrin Schopen, FZ Jülich
  - Michel Gerdes, DFN-CERT
  - Ana Alves, GÉANT Association
- Former and current members:
  - Urpo Kaila, CSC
  - Rolf Sture Normann, Sikt

The future

- SIG-ISM was created and approved in 2014
- Objective of this group work session:
  - Identify sections of the charter you want to change, discuss this within your group and present these afterwards for a discussion
  - Objectives, KPIs, Topics, collaboration with other SIGs, expectations
  - Meeting frequency, meeting type
- How would you like to get involved?

NREN (GÉANT) Community Programme

- National Research and Education Networks
- Security
  - TF-CSIRT
  - Transits
  - SIG-ISM



Presentations for GÉANT by Ana and Alf

Panel on Security Compliance

- Urpo Kaila, CSC
- Antonio Fuentes, RedIRIS
- Cynthia Wagner, RESTENA
- Tangui Coulouarn, DeiC

restena

réseau · sécurité · .lu

Fondation Restena

- *Compliance in Security*
  - What are we doing?
    - ISO27001 recertification in March 2025
    - includes all services within Restena
    - NIS2
  - Positive experience
    - Mostly reputation based
    - More requests for collaboration or requests on expertise
  - Negative experience
    - ...well where shall I start

Compliance at DeiC

- ISMS in principle mostly DKCERT: DeiC Compliance (GDPR, ISO27001, Statens Tekniske Minimumskrav, NIS2), DPO-service, crisis exercises
- ISO27001 “DeiC/i2, WAYF, DKCERT services, and the Research Network in accordance with the Statement of Applicability v.2.0” re-certification in August 2025. Scope: Hosting>Identity federation>DKCERT>research network
- NSIS: National Standard for Identiteters Sikringsniveauer (NSIS)
- NIS2: network, DIX, WAYF, datacentre inscope

COMPANY WITH
INFORMATION SECURITY
MANAGEMENT SYSTEM
CERTIFIED BY DNV
ISO/IEC 27001

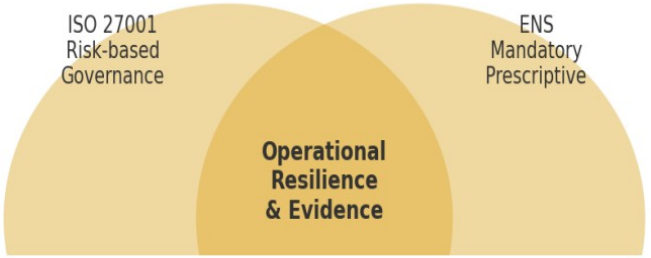
OIOSAML

Digitaliserings-styrelsen
NSIS-anmeldt
Betydeligt

NemLog-in

MitID

Real-World Compliance in RedIRIS



ISO 27001 provides a risk-based, international governance model.

ENS (Spain's National Security Framework) is mandatory and prescriptive, defining baseline measures for public institutions.

The Santa Claus Effect

When we are kids, we believe in Santa Claus.
Then we grow up, and we stop believing.

With compliance, it's the opposite.

When you're a technician, you don't really believe in compliance —
you think it's just paperwork, policies, and checklists.

But as you gain experience, you start to see how those contr
protect systems, improve coordination, and build trust.

That's when you start believing again —
and you understand that compliance isn't about bureaucracy
it's about resilience.

Key Challenges

Mapping ENS categories to ISO controls is easy - they share almost 85% of the requirements

High documentation workload and constant evidence maintenance.

Technician culture.

Annual audits with different auditors, each focusing on different controls and approaches

Limited technical staff and internal resources

Positive and Negative Aspects of Compliance (ISO27001 & ENS)

Positive

Improve service quality

Ensures consistent processes and higher reliability across all services, supported by clear SLAs and performance indicators

Enhances security monitoring

Provides better visibility, faster detection, and earlier response to incidents

Strengthens coordination and operacional procedures

Facilitates collaboration between teams and standardises response workflows.

Improves the decisión-making process

Enables data-driven and evidence-based decisions supported by audit trails

Positive

Supports NIS2 compliance alignment

Thanks to the alignment between ENS and NIS2, compliance frameworks prepare us for future obligations

Negative

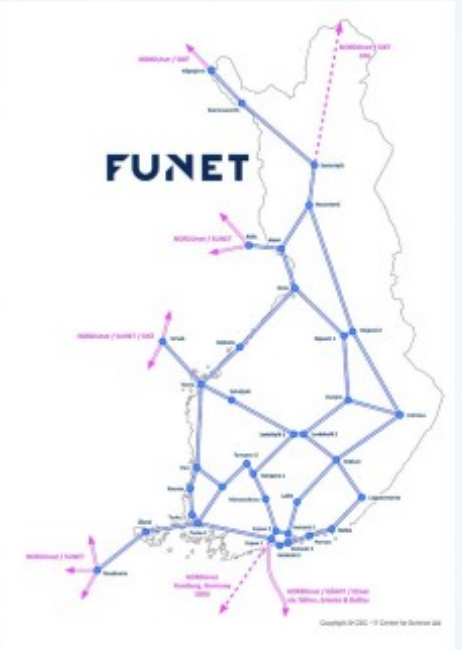
Ongoing maintenance

Requires continous updates, reviews, and audits to stay compliant

Resouce-intensive across the organization

Demands significant time and effort from multiple teams, often putting additional pressure on operational areas

CSC & FUNET



- CSC provides Finland's NREN, FUNET
  - Provides also HPC services ,data management, and digital services for research, education, and public administration.
  - A non-profit company, 700+ staff , operations started 1971
- Operators must comply to regulations of Finnish Transport and Communications Agency
  - Resilience and emergency preparedness required
- National certification for processing classified information
  - Scope: ISMS, specified premises
- ISO 27001 certification since 2013
  - Stared with Kajaani Datacenter
  - Current scope: Datacenter Operations, ICT and computing platforms, IaaS cPouta and ePouta, Long-term Preservation Service DPS, SAPA platform, Eduuni and Tiimeri collaboration platforms, LUMI hosting, Funet Miitti services, Funet Network and Secure Processing Environment (SPE4E) in Espoo and Kajaani
- NIS2 requirements covered by ISO 27001 SoA and incident reporting process

Open table discussions

Closing Day 1

- Sightseeing tour
  - Meeting at 19:00 at Puerta del Sol
  - Finish at the Restaurant for dinner
  - Group Photo
- Dinner (sponsored by RedIRIS), from 20:30
  - El Imparcial, Duque de Alba 4
  - Group Photo
- Tomorrow
  - Start at 09:30
  - Finish by 13:00 with a departing lunch being served until 14:00

Agenda for 2nd day

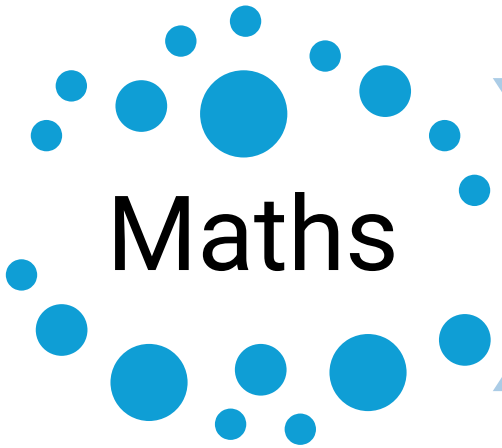
- Presentation by Nicole Harris, GÉANT
  - Security communications
- Panel on Security + A.I.
- Coffee break at 11:00
- 11:15 Presentation by CIRCL on their Vulnerability Lookup tool
- Open table discussions
- 13:00 lunch and goodbyes

Security Communications by Nicole

Panel on Security + A.I.

- AI: Mikolaj Dobski
- Privacy: Magdalena Rzaca
- Security: Andy Roebuck
- Network: Maria Isabel Gandia Carriedo

Mikolaj Dobski at the PSNC ICT Security Department Summary



Maths

- Partially Labelled, Imbalanced Data Streams with Concept Drift Detection (2012)
- Syscalls Anomaly Detection with NN (2010)

MCDM

Operator Tailored CTI (2016)

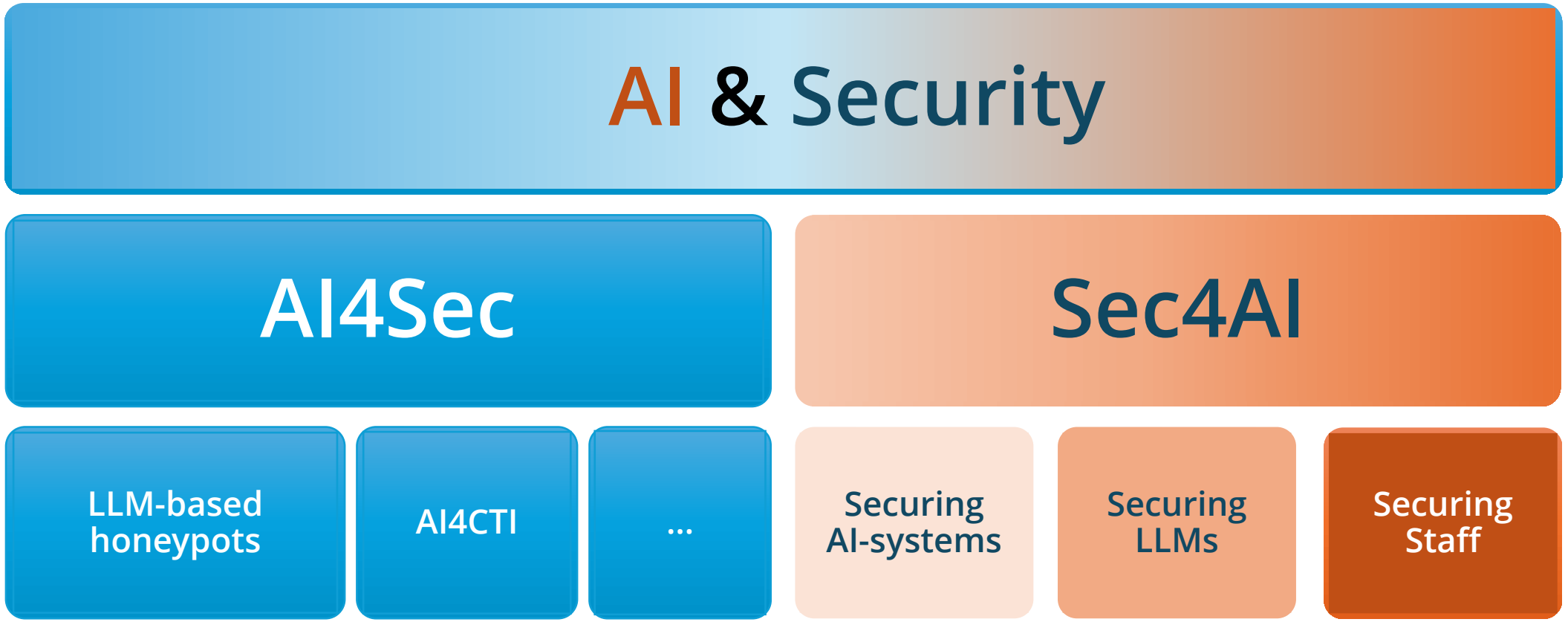
ML & Statistics

- IOT AuthN/Z Anomaly Detection (2016)
- SCADA IDS/IPS (2017)
- HPC & Forensics (2019)

LLMs

- Compliance
  - EOSC EU Node (2024)
- AI 4 Security
  - CTI NG Honeynet (2025)
- Security 4 AI
  - TBC

2025 AI & Cybersecurity Synergy at PSNC



AI & Security: The Missing Integration Layer

The Reality in Most Organisations:

- **Security**, **Privacy**, and **AI Governance** operate in **separate silos**
  → Different owners, languages, priorities, risk models.
- AI is often treated as a *tech add-on*, not a *risk-bearing system* requiring multi-domain oversight.

My perspective

More than 14 years of expierience

CIPP/E CIPM FIP, IAPP Chair

Certified ISO27001 Lead Auditor

Master's degree: Law/ Postgraduate studies: Cybersecurity management/ AI Master

I bring **all three domains together**: **AI Governance × Cyber/Security × Privacy**

Why? Because AI introduces **cross-cutting risks**:

Data leakage & model extraction

Bias, harmful outputs, autonomy risks

Lawfulness, GDPR/AIA compliance

Supply-chain/foundation model dependencies

Monitoring & incident response for AI behaviour

The Core Challenge

The biggest challenge is not AI itself — it's the organisational g

Bridging the silos is essential for safe, compliant, and trustwort

What Organisations Need

- A single **risk and governance** that merges:
  - Technical security controls
  - Data protection principles
  - AI-specific risk assessment & monitoring (AIA + DPIA + Safety Evaluation)
- Multidisciplinary teams and skills (legal × security × product × data).

ISO 42001 - Could it help?

- A framework to manage AI systems responsibly and ethically:
  - AI Management System = AIMS
- Focusses on key principles like:
  - Transparency
  - Accountability
  - Privacy
  - Security
  - bias mitigation
- Can be used to demonstrate compliance with EU AI Act
- Standardised risk based approach

AI & the Network: Towards Autonomous Networks

- Virtual agents (chatbots) help in configuration & the automation of repetitive tasks ✉ Zero touch
- Support decision making & planning infrastructure ✉ Self-planning / self-optimising /self governing
- Predicting & improving performance ✉ Self-ordering / Zero-trouble
- Predict and proactively prevent outages ✉ Self-healing / Self-repairing networks / Zero-downtime
- Closed loop automation ✉ Self-organising networks / Self assuring / Zero-touch operations
- Enhancing security, detection of unusual behaviour or security violations ✉ Zero-trust
- Minimise manual intervention, Automation ✉ Self-fulfilling / Self-assuring / Zero-touch operations
- Self service, zero wait

Vulnerability lookup tool (by CIRCL)

Open table discussion or presentations

Feedback

- Next meeting
  - TBD
- GÉANT Security Events
  - 2025
    - CLAW, December
  - 2026
    - Security Days, April

- Website: https://wiki.geant.org/spaces/SIGISM/overview

- Mailinglist: https://lists.geant.org/sympa/info/ism

- Coordinator
  - Annette Aylward, Annette.Aylward@geant.org

Thank You

Any questions?