



# LET'S START A NORDIC INFORMATION SECURITY MANAGEMENT NETWORK!

Urpo Kaila <urpo.kaila@csc.fi>

Rolf Sture Normann  
<rolf.sture.normann@uninett.no>

NTW2017, Kastrup 2017-09-12

# What is ISM\*?

- \*Information Security Management :
  - aims to ensure the confidentiality, integrity and availability of an organization's information, infrastructure, and IT services
  - is required by the stakeholders of an organisation
  - is owned by Senior Management (CEO, GM)
  - is reported typically to the CEO or to the General Manager
  - is focused on risk management and compliance
  - support and protect the company business
  - creates and ensures the Information Security Management Systems (ISMS) of the organisation
  - ensures trust
  - covers compliance, audits, and security related agreements
  - lead by a (chief) information security manager (CISO), Head of Security or similar

# Domains of ISM

- Security Management
- Access control
- Network security
- Cryptography
- Security architecture and models
- Operations security
  - Security awareness training
  - Incident response and coordination (CSIRT teams)
  - Logging
  - Malware protection
  - Change and configuration management
- Application and systems development security
- Physical security
- Compliance with laws, regulation and contracts
  - Audits and certifications
- Business continuity and disaster recovery

# How does ISM compare with Incident Response and Coordination?

## ISM

- Management
- Focus on data and services
- Information Security
- Processes
- Reports to top management
- Management/professional culture
- Aligned to business and governance
- Evolving communities ( GÈANT SIG-ISM, WISE)

## CSIRT\* activities

- Technical
- Focus on network and hosts
- Computer/Network Security
- Configurations
- Reports to community
- “Hacker culture”
- Semi-autonomous and aligned to cyber community
- Established communities (TF-CSIRT, FIRST)

\* Computer Security Incident Response Team

# What has been done so far at GÉANT SIG-ISM?

- Workshops (5 so far)
- Sharing Best Practices
- Site visits/Peer advise on implementing ISO/IEC 27001 for example
- White papers
- Guideline and tool for risk management
- Steering committee meeting regularly
- Liaison with WISE (<https://wise-community.org/>)



# How can we share best practices on ISM?

- Most NRENs and Research Infrastructures share similar challenges (Cyber compliance, GDPR, Cyber risks, Business risks)
- Sharing solutions and transferring skills in confidence can give huge benefits
  - Detailed security controls are typically not public
  - NDA combined with personal trust
  - The benefit lies in the details and controls which can be transferred
- Focus on one issue at time with clear deliverables
- Sharing benefits if the parties know and trust each other and share legal, cultural, financial and political value
  - -> **Regional groups**
  - -> **The Nordics**

# Charter for Nordic ISM Network

- **Scope: Share best practice on ISM for NRENs and research infrastructures in the Nordic**
- A by invitation network due confidentiality issue
- A Steering committee was formed on 2017-09-12 in Kastrup
- Reports to GÉANT SIG-ISM SC
- Rules for confidentiality
- Chair: Rolf Sture Norman, Uninett.no
- Current Steering committee: Ingimar Örn Jónsson, Juha Oinonen, Henrik Larsen, Robert Tofte, Urpo Kaila
- First task: expand membership to other relevant infrastructures
- Teleconferences quarterly with short status report from the Nordic Countries
- Possibly engage the Baltics later on, if there is interest?
- Aim to meet in person once per year, can be co-located with other events
- Possibly specific projects later on



## Contact, comments and more information:

Rolf Sture Normann <rolf.sture.normann@uninett.no> (chair)

Urpo Kaila <urpo.kaila@csc.fi>