



# SIG Information Security Management



3TH WISE WORKSHOP MIAMI


Alf Moens



## Whoami


- Corporate security officer SURF**
- Chair SIG-ISM**
- Board member SCIPR**
- Board member WISE**
- Member Géant Community Committee**
- ICT and security background with strong interest in privacy**




GÉANT


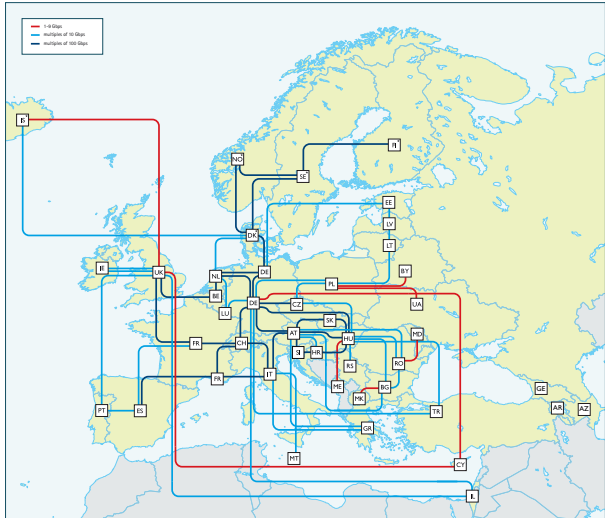
- **GÉANT is the leading collaboration on network and related infrastructure and services for the benefit of research and education**
- **an EC trusted partner for many years, as the coordinator of network projects co-funded by the European Union (EU).**
- **a member organisation with NRENs as members**

- **Research projects: GN4**
  - Network architecture
  - Network services
  - Trust and identity
- **Collaboration projects**
  - Several SIGs and taskforces;
  - MSP: NREN service delivery
  - Marcom
  - NOC
  - TF-CSIRT
  - SIG-ISM
  - TF-Storage
- **Spin offs**
  - REFEDS




www.geant.org

GÉANT's pan-European research and education network interconnects Europe's National Research and Education Networks (NRENs). Together we connect over 50 million users at 10,000 institutions across Europe.



GÉANT's pan-European network is funded by the GÉANT Project (GN4-1). This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 691567. The map shows topology as at October 2015. The GN4-1 partners are listed below.

## What is an NREN? Differs per country

SURF	universities	Research institutions	Professional education	AMC	others
4 entities	60 entities	20 entities	50 entities	8 entities	60 entities
300	650.000	5.000	300.000	60.000	40.000

Exclusive Network Service Provider

Federated Identity Management, community support

Added value services: certificates, filesender, DDOS protection

User requested services: Personal cloudstorage, virtual servers

Framework InformatieBeveiliging in het Hoger Onderwijs		Intranetversie december 2013				
Starterkit InformatieBeveiliging						
<b>Model Beleid InformatieBeveiliging</b> (update 2013/2014)						
Information Security Management System: ISO 27001:2013 (invoeren vanaf sept 2014?)						
HO Referentie Architectuur (SURF 2013)  Leidraad Informatie Beveiliging Architectuur	Baseline Informatie Beveiliging (Update 2014)	Leidraad AUP	Leidraad Classificatie (Update 2014 incl. LoA)	Leidraad Integriteit Code	Leidraad Functie-profiel (Update 2014 incl. FG)	Privacy
	Starterkit Identity Management	Starterkit RBAC	Starterkit Business Continuity Management	Leidraad veilig toetsen	IB in Projecten	Leidraad Responsible Disclosure (2013/2014)
	Leidraad Risico Management (RIK in 2014)	Leidraad Incident Management (Scirt)	Leidraad BYOD	CERT Starterkit	Cloud Normen-kader (SURF 2013/14)	Sourcing toolkit (SURF / CIO-beraad 2012)
	Veel implementatie voorbeelden van grote en kleine instellingen			Technische handreikingen (How-to's, FAQ's, etc.)		
	Normen-kader Informatie Beveiliging HO / SURFaudit (SURFaudit 2013)					
<div style="display: flex; justify-content: space-around; font-size: small;"> <span style="background-color: #92d050; padding: 2px;">Klaar (ToDo)</span> <span style="background-color: #cccccc; padding: 2px;">beheer bij derden</span> <span style="background-color: #ffff00; padding: 2px;">in Progress</span> <span style="background-color: #ffcc99; padding: 2px;">nog plannen</span> </div>						

## SIG ISM

### Géant SIG ISM

- Aimed at security officers
- Getting in control
- Information Security Management
- Incident management seen as part of security management

### Purpose

- Trust, on what basis?
- To certify or not to certify?

### Whitepapers

- information security management
- Risk management

### 2016:

- Expand the community
- Establish a Risk Register
- How to implement security management
- Anually

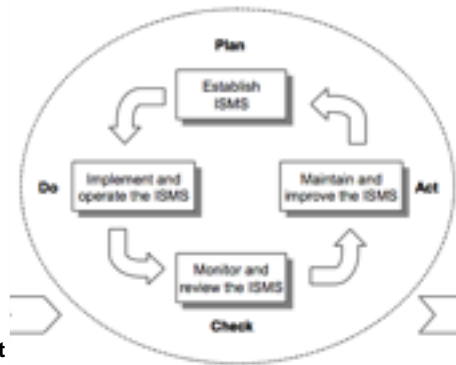


Figure 1 — PDCA model applied to ISMS processes

SURF NET

## NREN needs

### Strong CERTs

### Trust

Some are ISO 27001 certified or are working on it:

- Because they are a tld registry
- Because they deliver services to government
- Internal motivation: goals for quality management

With SIG-ISM we are joining forces on the subject of trust



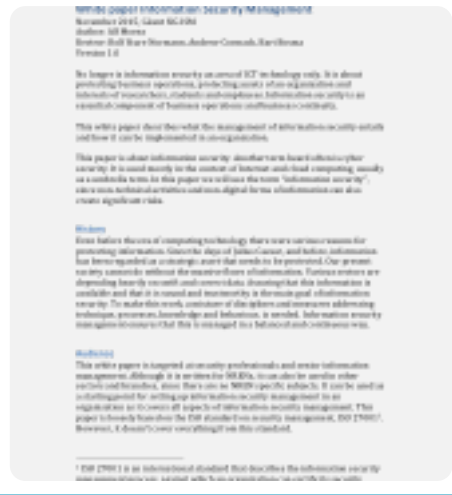
SURF NET

# Whitepaper on Security Management

High level paper on how to organise information security in you organisation

- Role and responsibilities
- Selecting standards

Full paper at:  
<https://wiki.geant.org/display/SIG/SM/SIG+ISM+white+paper+security+management>



# Whitepaper on Risk Management

High level paper on the setting up and maintaining a risk management proces for an NREN.

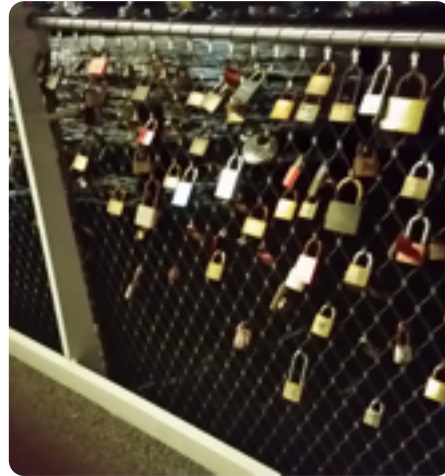
Paper in draft, publicly available in september 2016

About organisation and methods for establishing a risk register aimed at controlling risk and taken the right measures.



## Designing the Risk Matrix

- SIG ISM worked on 3 subjects of the Risk Matrix in her february workshop in Copenhagen
- Risks concerning hosted services
- Risks concerning People
- Risks concerning federated identity management systems
- First steps to a comprehensive risk matrix for an NREN
- Cooperate with WISE WG-SRA



SURF NET

## Outcome Copenhagen Workshop (work in progress)

### Hosted Services

- infrastructure complexity
- insecure software or infrastructures
- supplier
- incident detection
- trust/over-delegation

### People

- Economical loss/reputation
- Sickness
- Leaving staff
- Segregation of duties
- Policies
- Screening (lack of)

### Federations

- Declining (implicit) trust in growing federations
- Federation operator procedures and responsibilities
- Users cannot log in
- Cannot identify abuser/intruder
- Leak/abuse of personal information
- SP Data/Attribute profiles appropriate
- Protocol implementation vulnerabilities

SURF NET

**Allways be prepared  
For your next incident**



**From incident handling to security  
management**



Alf Moens  
Alf.moens@surfnet.nl  
www.surfnet.nl



WHAT **SURF** CAN DO