CSC

ICT Solutions for Brilliant Minds

Security in the Nordics

NeIC 2019 – Nordic Infrastructure for Open Science

CPH, 2019-05-16

Urpo Kaila <urpo.kaila@csc.fi>, Head of Security

CSC - IT Center for Science Ltd.

Introduction

Objectives of this Security Workshop

- To identify common needs to share and develop joint security measures among Nordic e-infrastructures.
- To identify requirements and solutions for security compliance to protect the infrastructures and sharing of data
- To cover fields of potential joint interests, such as:
  - Vulnerability management
  - Security assessments
  - Development of security skills
  - Ways to share critical information on security
- Please contribute with suggestions for joint security initiatives.
- Target audience: security professionals, service managers and persons responsible for external relations and liaisons at Nordic e-infrastructures.

What does security really mean?

- Hacker culture/Hacker meetings?
- Long passwords?
- Encryption?
- Restrictions?
- Control?
- Checking logs?
- Security policies?
- Patching vulnerabilities?
- Sharing information about incidents and data leaks?

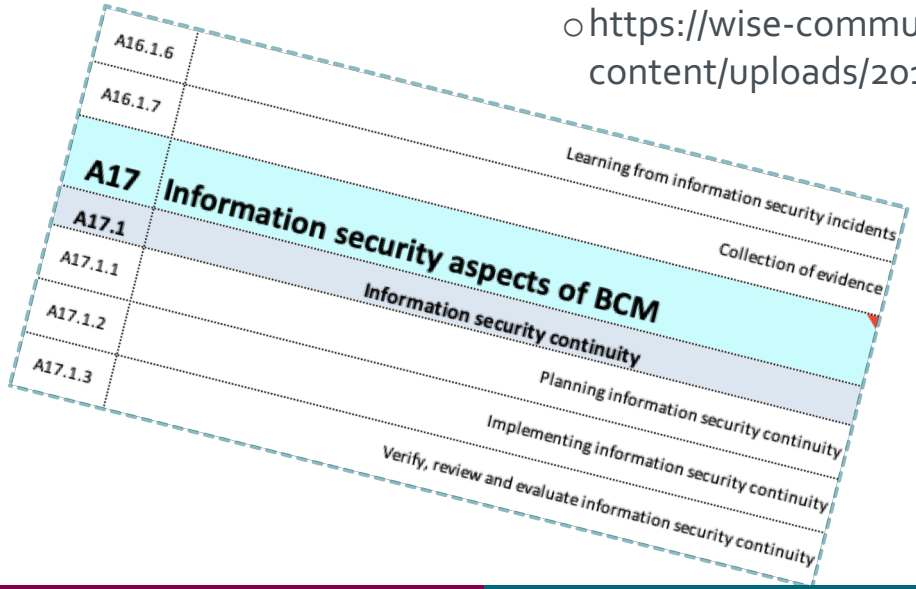
What is information security really about?

- Information security is about protecting assets (systems, data, services, and reputation) against risks with security controls
- Assets can (must) be protected to prevail their
  - Confidentiality: To prevent intentional or unintentional disclosure
  - Integrity: To prevent unauthorized modification and protect consistency
  - Availability: To protect reliable and timely access
- Information Security is
  - a building block of quality
  - a management responsibility
  - based on risk management and strategic objectives of the organisation
  - implemented by systemic security controls
  - the responsibility of all stakeholders

Risk Management

Ensuring Information Security

- Checklists
- Frameworks
- Standards
- *Reviews*
- *Scans and tests*
- *Audits*
- *Exercises*



- ISO/IEC 27001, 2700…
- SCI
  - https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf

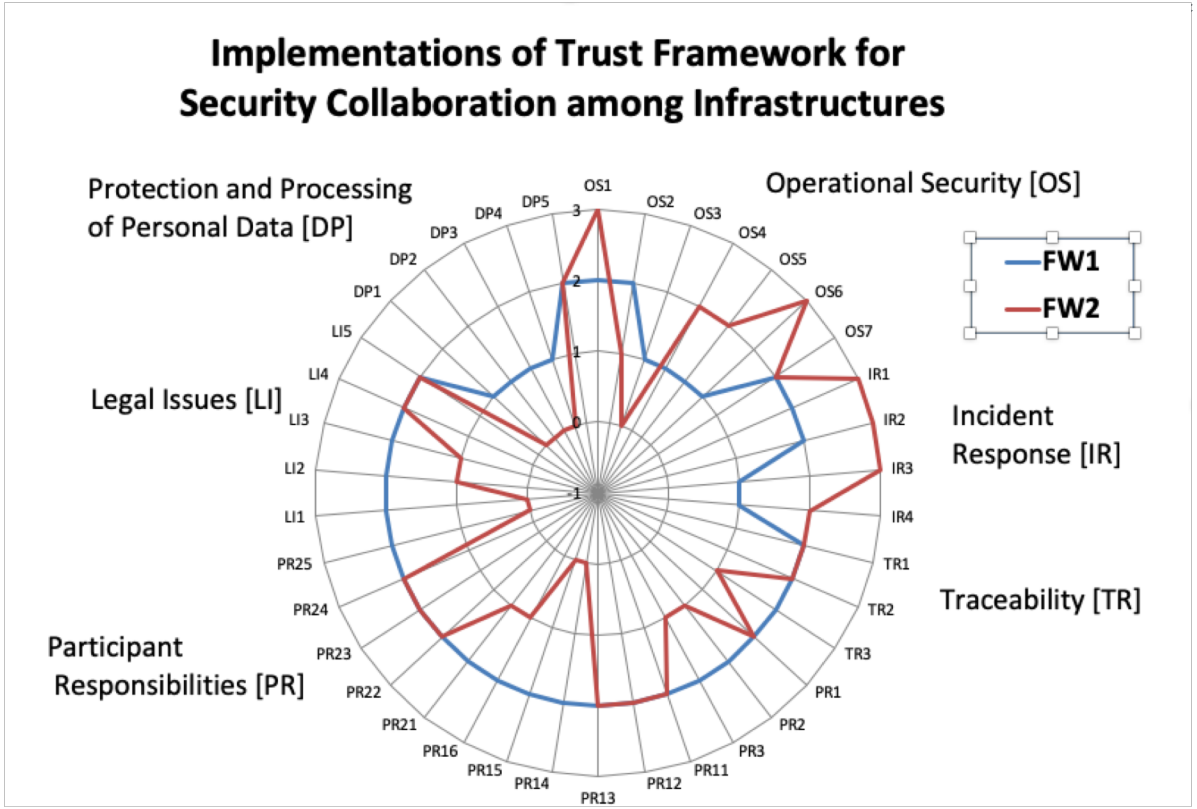
SCI - examples

3. Operational Security [OS]

Each of the collaborating infrastructures has the following:

- ❑ [OS1] A person or team mandated to represent the interests of security for the infrastructure
- ❑ [OS2] A process to identify and manage security risks on a regular basis
- ❑ [OS3] A security plan addressing issues, such as, authentication, authorisation, access control, physical and network security, risk mitigation, confidentiality, integrity and availability, disaster recovery, together with compliance mechanisms ensuring its implementation
- ❑ [OS4] A process to ensure that security patches are applied to operating systems, application software and firmware in a timely manner, and that patch application is recorded and communicated to the appropriate contact
- ❑ [OS++1] …

SCI Review tool



A NeIC Project Initiative 1/2

Cybersecurity PDI/ Nov 2018

- Identifying data, services, transfers, and systems to protect;
- Pooling of data risk for assessments between the parties;
- Joint adaption of a shared security framework;
- Joint comparison and development of security policies and guidelines;
- Sharing and developing common security tools and procedures;
- Penetration testing of shared services;
- Developing toolkit for security reviews;
- Implementing peer security reviews

A NeIC Project Initiative 2/2

Proposed tracks

- Policy definition and security management
- Security training
- Operational security
- Security reviews

This project initiative did not obtain enough support

- Why?

Another Nordic initiative from SuNet for NORDUnet Technical Workshop 2019

Topics to discuss in this workshop

Topics to discuss

- Would there be a real need and demand for joint Nordic security initiative within NeIC?
- If yes,
  - What would be the objectives?
    - Why?
    - What are the problems to solve/risks to mitigate?
  - What should be the deliverables?
    - Meetings? Reports? Policies? Guidelines? Solutions? Exercises? Reviews?
  - Who should be the stakeholders/participants?
    - Who would lime to commit/join?
  - How should the initiative be organised and resourced?
  - What would be the time span?
- Let's discuss at least all these topics and see if we could find areas of joint interest?

Conclusions

Conclusions of the workshop (TBD)

- Is there a need for a joint initiative?
- Objectives
  - ..
- Deliverables

- Stakeholders/participants

- How to organise?
- Time span?