



# Sharing best practices on risk management and the Risk Assessment working group (RAW-WG)

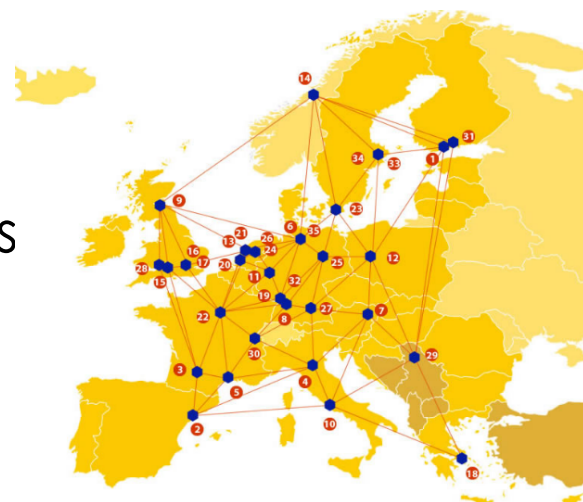
WISE@DI4R

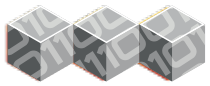
Digital Infrastructures for research  
28-30 September 2016, Krakow

Urpo Kaila  
EUDAT Security Officer  
urpo.kaila@csc.fi  
security@eudat.eu

# Sharing Best Practices on Risk Management

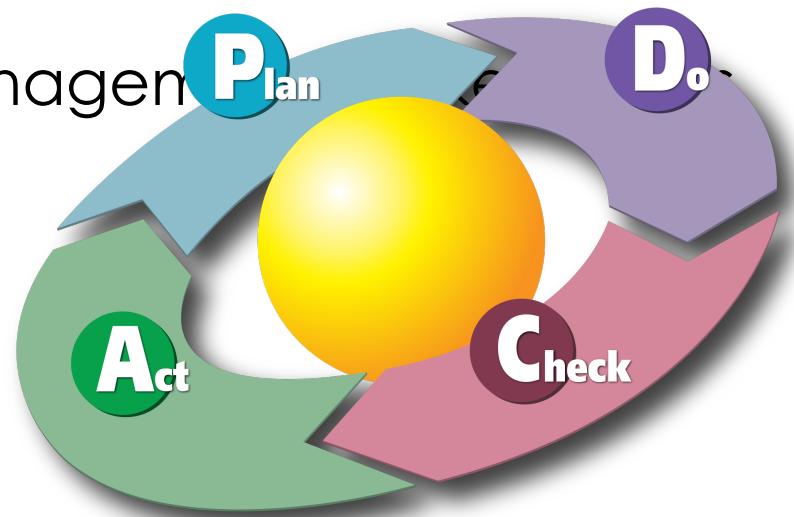
- Risk management is the starting point for information security
- Research infrastructures face very similar risks and can greatly benefit by sharing information about risks and methods for risk assessment and risk
  - Also the *controls* are often similar
- Within WISE a Risk Assessment working group (RAW-WG) was started
- RAW-WG had three joint teleconferences with WISE Security Review and Assessment working Group (SRA-WG)
- Sharing best practices in confidence between sites
- A presentation of Sharing Best Practices on Risk Management was held on 2nd GÉANT SIG-ISM Workshop, Feb 22, 2016





# EUDAT WISE WG's should cover core security domains

- Security Management
  - Policy sharing/harmonisation
- Risk Management
- Operational Security
  - Incident coordination
- Security training
- Security of Partner Management
- Security compliance
  - SCI2?
- (Technical security)



# Examples of sharing best practices: Risk types in CSC Risk Management Program

## Strategic risks

Risks that are often preceded by some (in principal) recognizable trends (e.g. economical recession). Mitigation is usually difficult

- ➡ Political risks
- ➡ Financial risks
- ➡ Personnel risks
- ➡ PR risks
- ➡ Environmental risks

## Operational risks

Risks that are often due to poor management. Well-defined processes and responsibilities can help.

- ➡ Service provision and development risks
- ➡ Contracting risks
- ➡ Supplier / subcontractor risks

## Damage risks

Risks that are due to accidental issues. Technical instruments and well-defined working practices can help.

- ➡ Property risks
- ➡ Information risks
- ➡ Person risks

# What next?

- ◆ A Survey?
- ◆ Sharing risks registers?
- ◆ Sharing tools and methods for risk management?
- ◆ How to share confidential information?
  - ◆ NDA?
  - ◆ F2F?
- ◆ Ways if work for WG's?
  - ◆ Teleconferences
  - ◆ Mailing list
  - ◆ Meetings
  - ◆ Objectives?
- ◆ How to review/audit Risk Assessment?