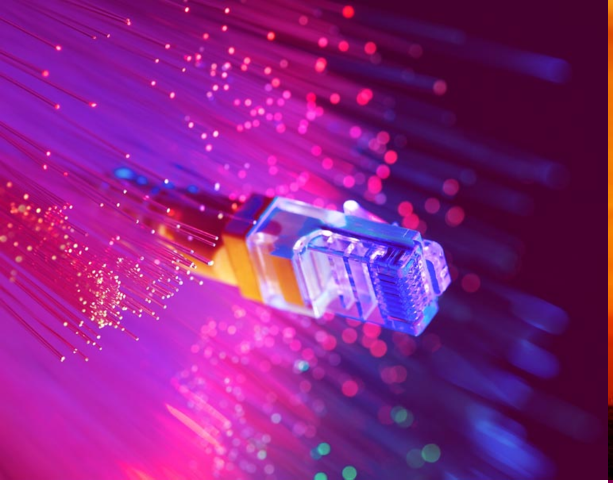


CSC

RAW Working Group
WISE @ Nikhef, www.wise-community.org
March 27- 29, 2017

Urpo Kaila, urpo.kaila@csc.fi

CSC – Suomalainen tutkimuksen, koulutuksen, kulttuurin ja julkishallinnon ICT-osaamiskeskus

Milestones

- Mission of RAW
- Current status of risk management at WISE stakeholders
- Best Practices/ Standards/Guidelines
- Issues with with Risk Management
- Required next steps
- RAW workshop

Mission of RAW

- This working group has the objective to provide e-infrastructures and their member organisations with guidelines on how risk assessments can be effectively implemented.
- As input, experience from organisations will be used. At the first WISE meeting some experiences were already presented, e.g. from XSEDE, UNINETT and EGI (https://www.terena.org/activities/ism/wise-ws/agenda.html).
- Some organisations may consider that information about specific risk assessments cannot be publicly provided and should be kept confidential.
- The working group should implement policies and procedures which enable, if needed, the exchange of confidential information among selected parties.

Current status of risk management at WISE stakeholders

You tell me:)!

Raise you hand if you do:

- ❑Regular risk assessments
- ❑Your risk assessments are comprehensive
- ❑Define risk ownership
- ❑Connect IT Risks and business risks
- ❑Your management is involved with risk management
- ❑You connect risk and security controls
- ❑You do follow ups to the risk assessment

Issues with with Risk Management

- Issues
  - Risk Management not done at all
  - No connection to strategic or operational risks
  - Fragmented RA’s
  - Missing management approval
  - Risk management a formality with no connections to operations or services
  - Risk ownership not defined
  - Missing connections between risks and controls
  - No follow ups
  - No methods
  - No audits

Activities

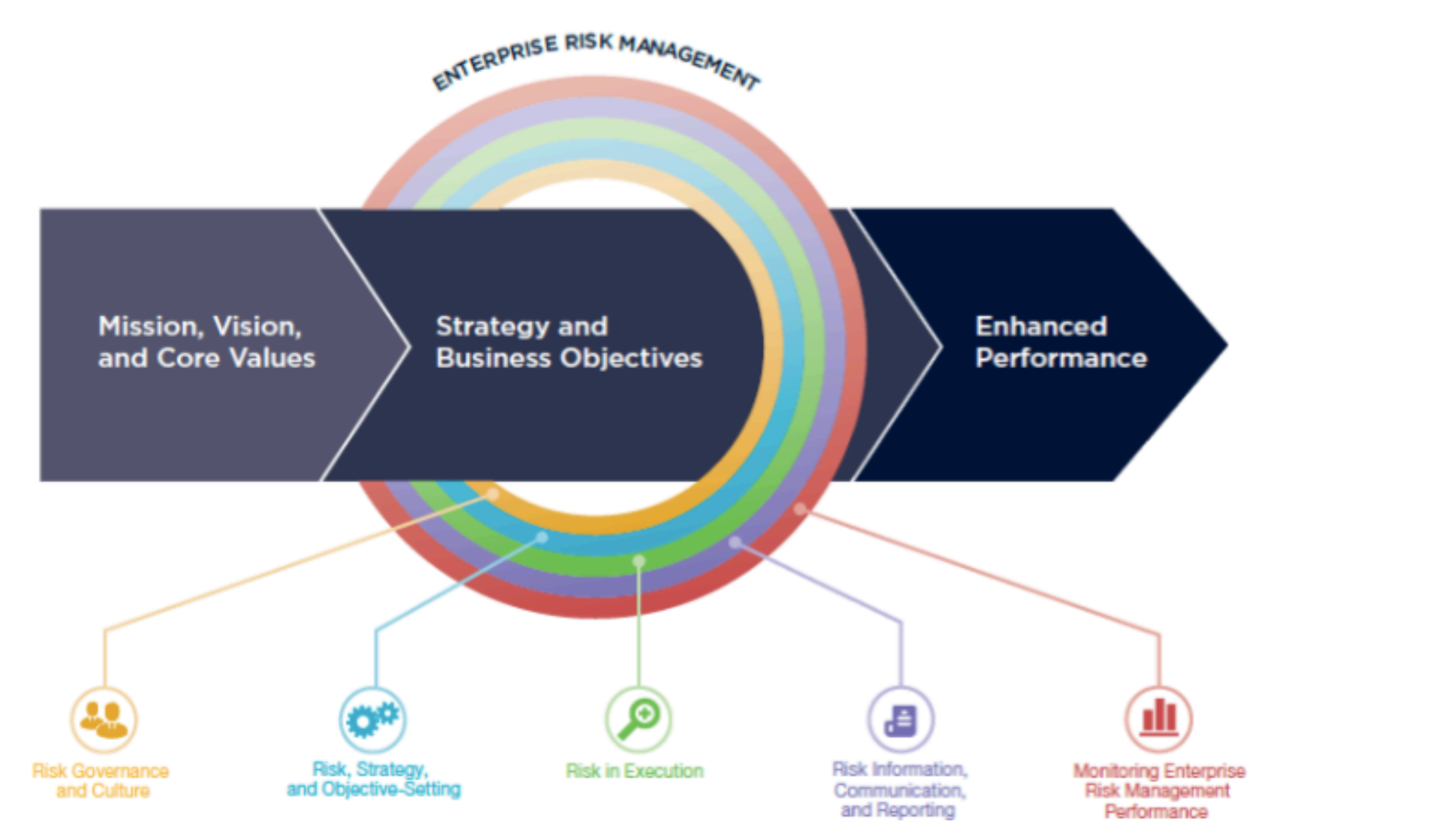
- Presentation at TNC17 as part of joint WISE presentation
- SC Meetings
- GÉANT SIG-ISM
  - Parallel work
  - Redefining ITSM basics/ Minimum requirements (an alternative to SCI)
- Audit tour of national universities (.fi)
- Preparing paper for SC conference

Best Practices/ Standards/Guidelines

- GÉANT SIG-ISM Whitepaper on Information Security Risk management (2016)
  - https://wiki.geant.org/download/attachments/51741496/Whitepaper%20Information%20Security%20Management%201.0.pdf
- ISO 3100
- NIST Technical series publications
  - 800-37, 800-53 (R 4),
- ENISA on Risk Management
  - https://www.enisa.europa.eu/topics/threat-risk-management/risk-management
- National Guidelines and Best Practices

Risk Management frameworks for various scopes

- COSO-ERM (-->)
- BIA
- PESTE
- Information Risks
- OWASP


ENTERPRISE RISK MANAGEMENT
Mission, Vision, and Core Values
Strategy and Business Objectives
Enhanced Performance
Risk Governance and Culture
Risk, Strategy, and Objective-Setting
Risk in Execution
Risk Information, Communication, and Reporting
Monitoring Enterprise Risk Management Performance

Objectives for RAW Workshop

- Create a practical and comprehensive risk management <u>template with instructions</u> to be shared among sites and infrastructures
- Subtasks, to to define best practices and practical examples for
  - Template
    - Scope of Risk Management
    - Risk Management methods
    - ISMS
    - Risk ownership
    - Procedures for follow up and continuous improvement of risk management
    - Framework to share information about risk management
  - A model implementation
    - Risk register