CSC

ICT Solutions for
Brilliant Minds

An update on best practices in risk management

8th SIG-ISM workshop
October 21-22, 2019, Zagreb

Urpo Kaila, urpo.kaila@csc.fi

Issues on risk management at NRENs and at their constituents

- Risk management is not implemented at all
- Risk management is undocumented
- Risk management is implemented as list of well known threats
  - Mitigation not defined
  - No risk ownership
- Management is not engaged in risk management
- No connection between risks and controls
- Business risks not identified
- BUT, risk management should be the starting point for information security

Reasons for issues on risk management

- The tradition of semi-independent role of experts in NRENs and at their constituents
- Low maturity in producing above-the-network services
- IT services often introduced first to support research and education of natural sciences, which seldom process confidential data or personal data,
- Implicit trust between actors in the NREN context
- Producing of IT services focused on technical implementations
- No direct monetary liabilities for risk events
- The standard frameworks for risk management are experienced as overwhelming

Challenges for risk management (at NRENs)

- GDPR
- Public-private partnerships
- Increasing dependence of commercial cloud services
- Big data
- The national implicit trust does not scale
- Emerging amount of human data
- Cyber risks
- Dependence on availability and integrity of outsourced data

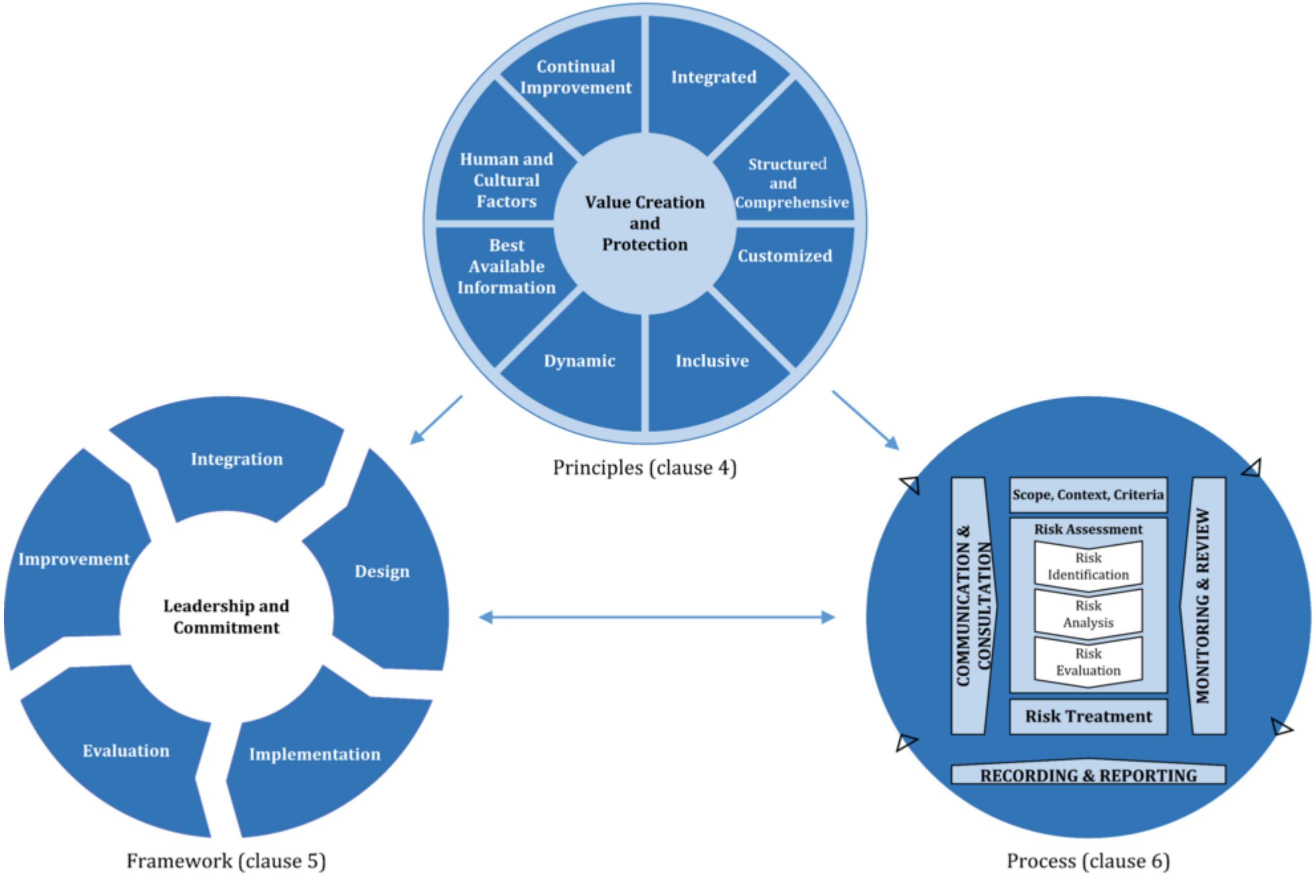
Suggestions on how to tackle the challenges on risk management

- Endorse a systemic approach to risk management
- Adapt well known best practices and standards for risk management from industry and business – but in a sustainable and evolutionary manner !
- Developing risk management practices for NRENs through networking
- Add trust to make it possible to disclose specific risks and controls in confidence among peers
- Update the WISE risk management framework

The ISO 31000:2018 standard for Risk management – Guidelines

- A simpler approach
- “increase the likelihood of achieving objectives, improve the identification of opportunities”
- Focus on leadership by top management
- Greater emphasis on the iterative nature of risk management

https://www.iso.org/iso-31000-risk-management.html
https://www.iso.org/news/ref2263.html



Principles (clause 4)

Framework (clause 5)

Process (clause 6)

Source: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

Other trends in Risk management

- Integrated risk management instead of top-heavy administrative GRC programs
  - Open
  - Business driven
  - Flexible
- No more massive risk sheets for senior management
- Gartner hype curve for risk management:
  - https://blogs.gartner.com/john-wheeler/practical-view-emerging-risk-management/
  - (click to open)
- Start your risk management program in an coherent way

Discussion and next steps