

Risk Management at CSC – Sharing Best Practices

2nd GÉANT SIG-ISM Workshop

Urpo Kaila, Head of Security, Feb 22, 2016



CSC-IT CENTER FOR SCIENCE

Overview

- About CSC
- CSC ISMS
- CSC Risk Management Program
- Experiences and Learning's
- Next Steps

About CSC

- CSC - IT Center for Science Ltd. is a state-owned, non-profit company administered by the Ministry of Education and Culture in Finland
- CSC offers IT services for research, education, culture, and government
- CSC provides Finland's widest selection of scientific software and databases and Finland's most powerful supercomputing environment that researchers can use via the Funet network
- www.csc.fi



- Founded in 1971 as a technical support unit for Univac 1108
- CSC connected Finland to the Internet in 1988
- Reorganized as a company in 1993
- CSC's datacenter in Kajaani started in 2012
- Turnover 32,7 milj. euros in 2014



270
Employees

Facilities in Espoo and Kajaani



Keilaniemi, Espoo



Renforsin Ranta, Kajaani

Services

- Computing Services
- Research Information Management Services
- Funet Network Services
- Education Management and Student Administration Services
- Identity and Access Management Services
- Datacenter and Capacity Services (IaaS)
- Training Services
- Consultation and Tailored Solutions



- Ministry of Education and Culture
- Other ministries and state administration
- Higher education institutions
- Research institutions
- Companies

About Customers

- About 700 active computing projects
 - 3000 researchers use CSC's computing capacity
 - 4250 registered customers
- Funet connects about 80 organizations to the global research networking infrastructure
 - Universities and polytechnics
 - Total of 372 000 end users
- Haka-identity federation covers 95% of universities and higher education institutes (287 000 users)
 - Haka federation and identity management system is a gateway to over 160 services
 - Over 20 million registrations in Haka services 2014
- CSC's Training Services
 - over 3000 participants in 2014
 - 150 course days

CSC is a trustworthy partner



- CSC complies to requirements and best practices on information security
 - national requirements (Raised Information Security Level)
 - audited several times
 - international standards
- CSC has been awarded the ISO/IEC 27001 information security certificate
 - The certificate covers CSC's Data Centers, ICT platforms, Preservation Services and IaaS Cloud Services
- The certification ensures that CSC has the ability to manage, lead and continuously improve the information security of its services



ISO/IEC 27001

Main elements in CSC ISMS

- Security policy
- Security team
- Risk management programme
- Incident management guideline
- Production catalogue
- Other security guidelines
- Business plans and disaster recovery plans
- Privacy policy and guidelines
- Audit plan
- Security agreement procedure
- Security and awareness training
- Procedures for management reviews

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

CSC Risk Management Program

Strategic risks

*

- ➔ Political risks
- ➔ Financial risks
- ➔ Personnel risks
- ➔ PR risks
- ➔ Environmental risks

Operational risks

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

Damage risks

**

- ➔ Property risks
- ➔ Information risks
- ➔ Person risks

* Risk owners: CSC Board and CSC Senior Management

** Risk owners: CSC Group Managers

Risk ownerships and mitigation controls defined in Appendix for detailed Risks

Risk = Impact (1-5) x Probability (1-3)

ISMS/2Kaila

Risk Value

[1-5] = LOW

[6-9] = MEDIUM

[10-14] = HIGH

[15] = UNACCEPTABLE

Input for CSC level risk assessment

- CSC Directors (strategic risks)
- Managers and administrators
- Auditors and Comptrollers
- Internal audits
- Internal technical reviews
- External information (security partners etc)

Required Risk assessments in CSC internal BCPs



- **List the most important risks (3-9) endangering the service**
 - **List only the service specific risks in addition to CSC Corporate level risks**
- **List the most important (3-9) existing and proposed controls for risk mitigation**
- **List the expected and worst-case impact scenarios (5-10)**
- **Definition of normal operations, incident and disaster (use metrics if possible)**

Fields in CSC internal risk management tool

- **Root cause of risk event**
- **Risk event**
- **Consequences**
- **Preventive actions**
- **Impact**
- **Probability**
- **Risk**
- **Action (risk) owner**
- **First aid**
- **Approved Risk Residual**
- **Related SoA Control**



CSC'S risk metrics for 2014




Risk Type	High Risks	All Risks
Strategic Risks	5	24
Operative Risks	2	34
Damage Risks	2	26

Developing Risk Assessment



Risk identification	Mitigation measures
Strategic	
Operational	
Damage	

A large blue 3D-style arrow pointing from the bottom right towards the "Operational" row of the table.

Experiences and learning's of CSC risk management programme

- The programme works pretty well!
- Through RM in BCP's we have succeed to cope with operational and damage risks in a sensible way
- The ERM/Strategic part emphasise in a good way the role of and governance related responsibilities of Senior management and the Board of Directors
- Good cooperation with the comptrollers
- Incident metrics and security reviews (both technical and management audits) are a good input for risk assessment
- Compliance enforce risk management
- The process is still very manual



Summary and next steps

- Proper risk management is a necessary foundation for security and governance
- Excellent input and feedback from technical experts
- You should design a risk management framework that suits your organisation
- Compliance requirements with ISO/IEC 27001 can sound a bit hard in the beginning
- Good risk management creates a solid and transparent security context for all stakeholders in your organisation
- We should do a survey of risk management practices among peers
 - I can volunteer to implement this