CSC

ICT Solutions for Brilliant Minds

Handling Security Risk in EOSC

SIG-ISM /WISE Joint Workshop

2021-10-26

Urpo Kaila <urpo.kaila@csc.fi>

Agenda

- Risk Management – What, how, and why?
- Different types and catergories of risks
- Risk assesment vs Risk Management
- Risks Management in EOSC
- Current risks
- Discussion

Risk Management – What, how, and why?

- ISO 31000:2018:
- Risk is the "effect of uncertainty on objectives"
  - An effect is a deviation from the expected. It can be **positive**, negative or both, and can address, create or result in opportunities and threats
  - Objectives can have different aspects and categories, and can be applied at different levels.
  - Note 3 to entry: Risk is usually expressed in terms of **risk sources**, potential **events**, their **consequences**, and their **likelihood**
- **Information security should be risk-based**
  - Not based on current tools or current practices

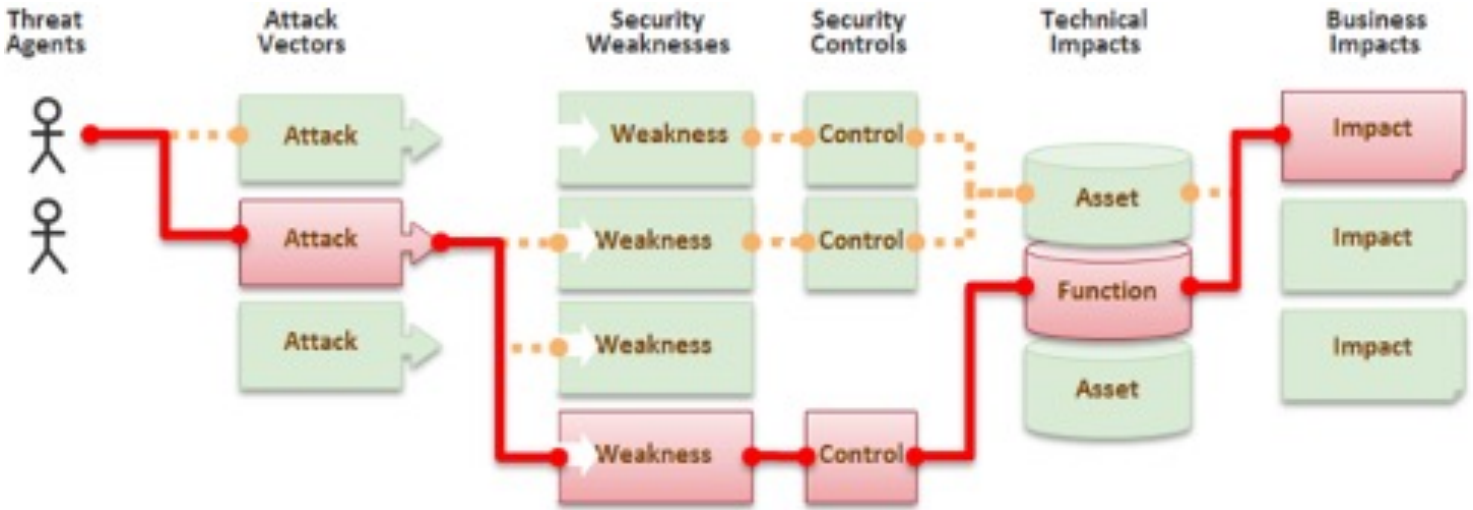
Different categories of risks and related roles (1/2)

- Strategic risks – Senior management
  - Political
  - Legal
  - Financial
  - Trust and reputation
  - Personell
  - (Data protection)
- Operational risks – Operational management
  - Service provisioning
  - ….

Different categories of risks and related roles (3/2)

- Operational risks
  - Service provisioning
  - Agreements/Supplier relations
- Damage risks – Operational teams
  - Property
  - Information security
  - Safety

Information security risks according to OWASP (simplified version)

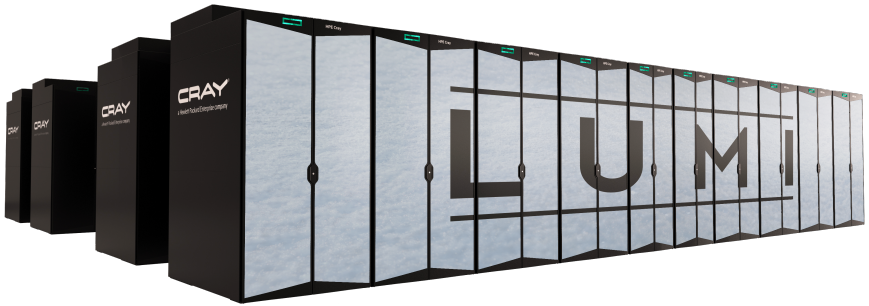


https://owasp.org/www-project-top-ten/2017/Application_Security_Risks

HPC environments as attack target

- Supercomputers constantly targeted since the dawn of computing
- Most of the "attacks" is just noise
- Anything exploitable will always be compromised very soon
- Increased complexity in service layers, architecture, technologies, and trust structures will increase exposure surface
- Attacker profiles
  - 'Script kiddies', malicious individuals
  - Security experts, black hats, vulnerability exploiters
  - Cyber Security Agencies
  - Malicious insiders

LUMI: one of the fastest supercomputers in the world



- LUMI is a **HPE Cray EX** supercomputer manufactured by **Hewlett Packard Enterprise**
- Peak performance will be over **550 petaflop/s, which** makes the system one of the world's fastest supercomputer

1 system

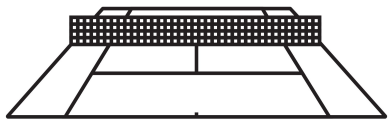
550 Pflop/s

Peak Performance

Computing power equivalent to

1 500 000

Modern laptop computers



Size of a tennis court

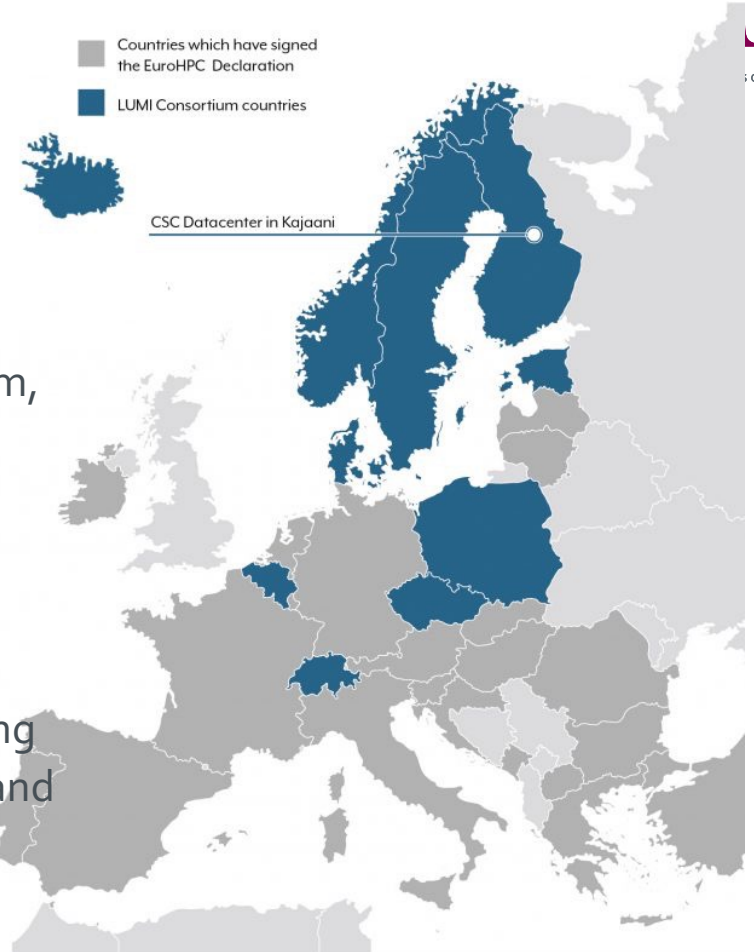
Modern platform for

High-performance computing, Artificial intelligence, Data analytics

Based on GPU technology

LUMI Consortium

- Unique consortium of 10 countries with strong national HPC centers
- LUMI consortium members are Finland, Belgium, Czech Republic, Denmark, Estonia, Iceland, Norway, Poland, Sweden and Switzerland
- The resources of LUMI will be allocated per the investments
- The 50% share of the EuroHPC Joint Undertaking (JU) will be allocated by a peer-review process and available for all European researchers
  - JU pools EU and national resources in (HPC)



Common risks in supercomputing

- System compromise
  - Compromised user account or privileged account
- Data or service not accessible
  - Data accessible without adequate authorization (exposure to vulnerabilities)
  - Data is erased, corrupted or modified without adequate authorization
- Technology risks (example: brute-forcing with quantum computing)
- Risks on liabilities (users and third parties)
  - Risk related to rights of data subjects (GDPR)
  - IPR
- Unauthorised use or abuse
- Loss of trust, reputation damages

Sounds great but does it work?

- It is about data, not about computers
- When (not if) an incident occurs you must have everything in place
  - Skilled and motivated people
  - Clear roles and responsibilities, teamwork
  - Capacity for forensics and recovery
  - Procedures and contacts to stakeholders and incident response teams
  - Crisis communication plan
- Ensure seamless communication and cooperation between roles
  - Administators and user support/communication
  - Management, legal, and operations teams must interact
  - Stakeholders and peers

Information Security Risk Management

- Information security risk management is a proactive approach to security
- A framework for management accountability
- A tool to connect business, services, service components and technical components
- To avoid and and mitigate incidents you need both security and risk management
- We need to both technical and administrative security controls
- To apply security controls we need both a plan and a process
  - It is not enough to apply security controls in random

How can we do risk management together?

- We should use joint tools and templates

- Risk management should be a regular and recurring activity in EOSC
  - Required by the reviewers as well

- We need a good flow between DevOps, security and risk management

WISE Risk Management template - Adapted for an assessment of the principle of the EOSC catalogue

						1-4	1-4	1-16				
Threat	STRIDE type of Threat	Existing controls	vulnerabilities/ weaknesses	Risk targets	Description of Impact	Impact	Likelihood	Risk	Risk owner	Approved residual risk	Actions items	Reviewed

WISE Risk Management Template

- https://wiki.geant.org/display/WISE/RAW-WG

Based on the WISE Risk Management template - Adapted for an assessment of the principle of the EOSC catalogue

Completed: 2020-06-30 (draft)

Risk Assessment of the EOSC catalogue

Threat	Selected for this Risk Assesment (Yes/No)	STRIDE type of Threat	Existing controls	Still exisiting vul weaknesses
Threats to Catalogue on Web Page				
Web page itself hacked to include services which are not authentic/approved	Yes	**S**	Run by EGI/EOSC, AAI, web software kept up to date? Risk Assesment	No detailed asses carried out, both i used or how it is c
Web page itself hacked to modify other information on the web page		**T,D**	Run by EGI/EOSC, AAI, web software kept up to date?	
Threats resulting from Marketplace software				
Market place/database/ticketing system behind it hacked to include services which are not authentic/approved	**N/A**	**S**	Run by EGI/EOSC, AAI	
Market place/database/ticketing system behind it hacked to modify or disclose	**N/A**	**T,D, I**	Run by EGI/EOSC, AAI	

ISM Security Controls and Risk

See:

- https://confluence.egi.eu/pages/viewpage.action?spaceKey=EOSC&title=ISM+Security+Controls+and+Risk
- https://confluence.egi.eu/display/EOSC/ISM6+Controls
  - Review of the procedure
- https://rt.egi.eu/rt/ and click on ISM-controls in the box on the right.

EOSC-Future Risk assessment frameworks

- Evolve and align an information security risk assessment framework for EOSC services
- Federated evolution of the WISE SCI framework and a multi-tier maturity model
- Inclusive of data security and data protection
- Information Security Management (ISM) risks play out differently depending on the assets involved, the sensitivity and amount of (personal) data processed and the impact incidents may have on the other services.

Information Security Risk Management in EOSC-Future

- Asset inventory must be comprehensive and up-to-date
- Asset owners must identify risk related to their assets
- Risk assessment should be performed periodically, based on up-to-date information on changes. ,vulnerabilities and threats
- Together with other experts, identify, plan, implement and document information security controls to treat risks