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
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 management.

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.
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

<table>
<thead>
<tr>
<th><strong>Strategic risks</strong></th>
<th><strong>Operational risks</strong></th>
<th><strong>Damage risks</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Risks that are often preceded by some (in principal) recognizable trends (e.g. economical recession). Mitigation is usually difficult.</td>
<td>Risks that are often due to poor management. Well-defined processes and responsibilities can help.</td>
<td>Risks that are due to accidental issues. Technical instruments and well-defined working practices can help.</td>
</tr>
<tr>
<td>- Political risks</td>
<td>- Service provision and development risks</td>
<td>- Property risks</td>
</tr>
<tr>
<td>- Financial risks</td>
<td>- Contracting risks</td>
<td>- Information risks</td>
</tr>
<tr>
<td>- Personnel risks</td>
<td>- Supplier / subcontractor risks</td>
<td>- Person risks</td>
</tr>
<tr>
<td>- PR risks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Environmental risks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


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?