SCI status PRACE

Jules Wolfrat, SURFsara

EGI-EUDAT-PRACE security workshop, Linkoping, Sweden, 8 October 2013

CAPACITIES

e-infrastructure

SCI status PRACE

- Members of the PRACE Security Forum have been involved in the SCI discussions from the start (Vincent Ribaillier, Ralph Niederberger, Jules Wolfrat)
- Security self assessments by PRACE sites
  - Based on SCI document
  - Just started, also for PRACE as an infrastructure. Will be scheduled for next months.
  - Must improve the level of trust
  - Experiences will be used to provide feedback to SCI

PRACE assessment

- PRACE is not an homogeneous infrastructure. Tier-0 sites are governed by PRACE RI and Tier-1 sites by consortium agreement of IP projects.
- Tier-0 users sign a contract with a Tier-0 site and Tier-1 users with a Tier-1 site. The latter is used to give access to other Tier-1 sites, so important for Tier-1 sites to know what users sign.
- Tier-1 users all sign the same AUP. For Tier-0 users a draft AUP has been defined, waiting for acceptance.

SCI maturity levels

- Level 0: Function or feature not implemented
- Level 1: Function or feature exists, is operationally implemented but not documented
- Level 2: Function or feature is comprehensively documented and operationally implemented
- Level 3: Function or feature implemented, documented, and reviewed by an independent external body

PRACE assessment (2)

- Most items cannot be answered because we don't have a PRACE wide policy. Important that sites assess the requirements.
- We don't have user communities, although we have PIs who have responsibilities for their project and the use by other users in that project
- Documents and information: Security Forum mandate (high level document), AAA administration guide, PRACE wiki, PRACE LDAP, Tier-1 AUP
  - Level 2 has been determined on above documents and information

PRACE level 2

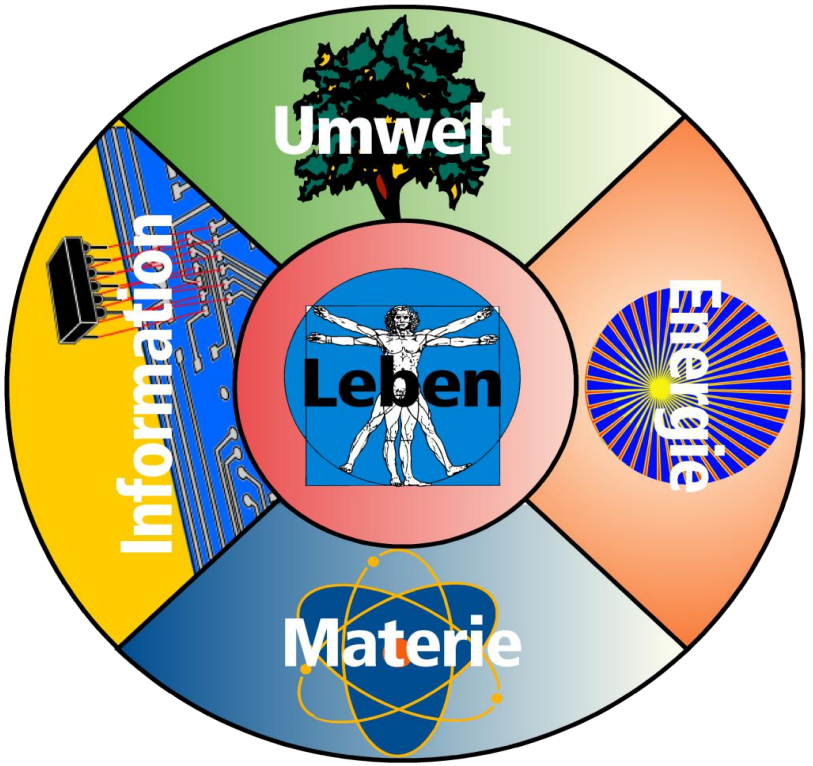
- Function or feature is comprehensively documented and operationally implemented
- OS1.2 - Authorisation
- OS6 - Contact Information (6.1, 6.2 and 6.3)
- IR1.1 - Contact Service Providers
- IR1.2 - Contact Resource Providers
- IR2.1 - IR Roles & Responsibilities
- IR2.5 - IR Communication Tools
- IR3.1 - Internal Collaboration
- PR1 - AUP (only Tier-1)

PRACE assessment (3)

- Gaps
  - Several Operational Security (OS) requirements (assumed in place at sites, but must be assessed)
  - IR2 - Incident Response Procedure must be better defined
  - TR1 – Traceability: must be documented
  - Tier-0 AUP pending
  - Participant Responsibilities [PR] - Resource Providers and Service Operators: not documented
  - Legal Issues: not known because contracts are not assessed
- Priority is to increase awareness and knowledge of site policies and procedures

Forschungszentrum Jülich GmbH (FZJ)

- founded in December 1956
- 5 main research areas (environment, energy, material, information, life science)
- 4000 – 5000 members of staff
- 42 institutes
- 2001: 241 patents granted
- 50 Mio. € third-party funds

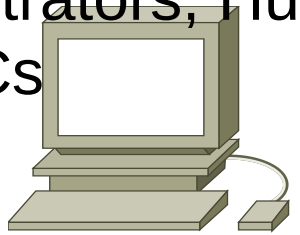


Network participants

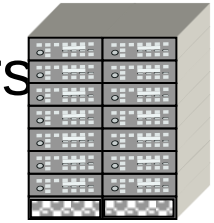
- ~17000 connected systems / 300 IP sub nets

600 Routers, Switches, Bridges, Concentrators, Hubs

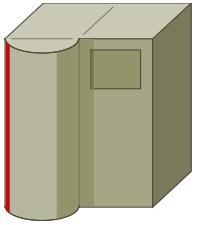
12000 Workstations, PCs



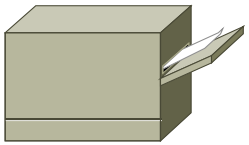
different PC-Clusters



different HPC systems



800 printers



Assessment FZJ

- Mature Security organization
- SCI requirements almost all on level 2 (Function or feature is comprehensively documented and operationally implemented)
  - IR collaboration and Traceability can be improved
- Documents however are all in German, can be a problem for foreigners (do they understand what they sign?). No translation available
- Documents are not public. This was never considered, but can be discussed.

SCI feedback

- Availability of policies and procedures is discussed, no minimum set of requirements for the policies and procedures
  - Can we add these, e.g. based on documents from security bodies, e.g. national security organizations?
  - Use ISO 27001 references?