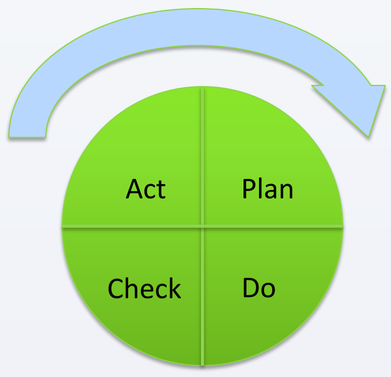
WLCG Security: A Trust Framework for Security Collaboration among Infrastructures

K.Chadwick[1], I. Gaines[1], D. Groep[2], U. Kaila[3], C. Kanellopoulos[4], D. Kelsey[5], J.Marsteller[6], R. Niederberger[7], V. Ribaillier[8], R. Wartel[9], W. Weisz[10], J. Wolfrat[11]
([1]FNAL, [2]Nikhef, [3]CSC, [4]GRNET, [5]STFC, [6]PSC, [7]FZ Jülich, [8]IDRIS, [9]CERN, [10]Univ of Vienna, [11]SURFsara)

IT Security and Trust

Risk Assessment -> Security Plan -> Security Controls -> Security Policy and Procedures



ISO 27001 ISMS

Common threats & shared users

CSIRT teams collaborate on Security incidents

The SCI group

- SCI = "Security for Collaborating Infrastructures"
- A collaboration of IT security officers from DCIs, including EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, and XSEDE
- Many specifications of Security best practice (ISO 27001, NIST 800-53, …) but not directly applicable to a distributed infrastructure with many management domains
- Building a Security Policy Framework
  - Enable interoperation (security teams)
  - Manage cross-infrastructure security risks
  - Develop policy standards
- Documents best practice
- Builds trust between the infrastructures

- **Future plans**
  - Infrastructures to do Self Assessment
  - Seek feedback from Infrastructure management
  - Improve SCI document

The SCI document

SCI: A Trust Framework for Security Collaboration among Infrastructures

Aims:
"A framework to enable interoperation of collaborating Distributed Computing Infrastructures (DCIs) with the aim of managing cross-infrastructure operational security risks and to build trust and develop policy standards for collaboration"

Areas covered:
Operational Security
Incident Response
Traceability
Participant Responsibilities
- Individual users
- Collections of users
- Resource providers, service operators

Legal issues and Management procedures
Protection and processing of Personal Data/Personally Identifiable Information

Text example extracted from the SCI document:

Imperative that an infrastructure has an organised approach to addressing and managing events that threaten the security of resources, data and overall project integrity.

Each infrastructure must have:

[IR1] Security contact information for all service providers, resource providers and communities together with expected response times for critical situations.

[IR2] A formal Incident Response procedure, which must address roles and responsibilities, identification and assessment of … *(text continues)*

Reference: http://www.eugridpma.org/sci/

Further information from: David.Kelsey@stfc.ac.uk

Assessment of maturity

Level 0: Function or feature not implemented

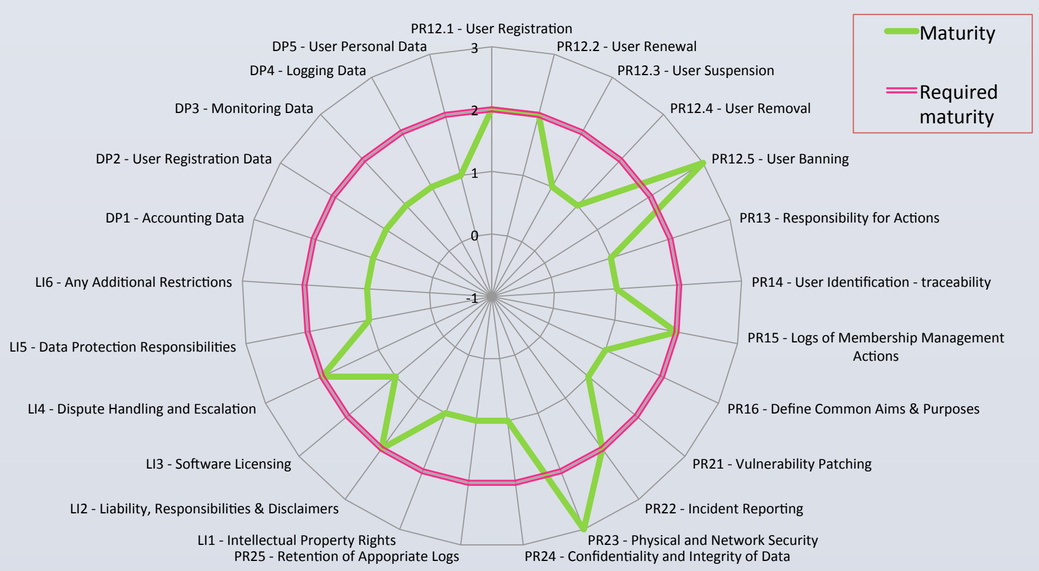
Level 1: Function or feature exists, is operationally implemented but not documented

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

Infrastructure Name:	<insert name>					
Prepared By:	<insert name>			On Date:	<insert date>	
Reviewed By:	<insert name>			On Date:	<insert date>	
Incident Response [IR]	**Maturity**	**Evidence (Document Name and/or URL)**	**Version Number**	**Document Date**	**Document Page or Section Number**	**Comments**
IR1 - Contact Information						
IR1.1 - Contact Service Providers						
IR1.2 - Contact Resource Providers						
IR1.3 - Contact Communities						
IR1.4 - Expected Response Times						
IR2 - Incident Response Procedure						
IR2.1 - IR Roles & Responsibilities						
IR2.2 - IR Identification & Assessment						
IR2.3 - IR Minimizing Damage						
IR2.4 - IR Response & Recovery						
IR2.5 - IR Communication Tools						
IR2.6 - IR Procedures						
IR3 - IR Collaboration						
IR3.1 - Internal Collaboration						
IR3.2 - External Collaboration						
IR4 - information Sharing Restrictions						

SCI Assessment of a fictitious computational Infrastructure



Example spider diagram of a fictitious assessment.
Graph kindly created and provided by the
CSC Head of Security, Mr. Urpo Kaila <urpo.kaila@csc.fi>.