Security for Collaboration among Infrastructures (SCI)

WISE COMMUNITY

EUGRIDPMA- 2021-02-08

Ian Neilson (STFC-RAL, UK Research and Innovation)

Uros Stevanovic (Karlsruhe Institute of Technology)

https://wise-community.org

In collaboration with and co-supported by EnCo (GN4-3)

Security for Collaborating Infrastructures (SCI-WG)

- A collaborative activity of information security officers from large-scale infrastructures
  - EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, XSEDE, HBP…
- Grew out of EGEE/WLCG JSPG and IGTF –from the ground up
- We developed a *Trust framework*
  - Enable inter-operation (security teams)
  - Manage cross-infrastructure security risks
  - Develop policy standards
  - Especially where not able to share identical security policies

WISE SCI Version 2

- Aims:
  - Involve wider range of stakeholders
  - GEANT, NRENS, Identity federations, …
  - Address any conflicts in version 1 for new stakeholders
  - Add new topics/areas if needed (and indeed remove topics)
  - Revise all wording of requirements
  - Simplify!
- SCI Version 2 was published on 31 May 2017
- https://wise-community.org/sci/

WISE COMMUNITY

A Trust Framework for Security Collaboration among Infrastructures

SCI version 2.0, 31 May 2017

L Florio[1], S Gabriel[2], F Gagadis[3], D Groep[2], W de Jong[4], U Kaila[5], D Kelsey[6], A Moens[7], I Neilson[6], R Niederberger[8], R Quick[9], W Raquel[10], V Ribaillier[11], M Sallé[2], A Scicchitano[12], H Short[13], A Slagell[10], U Stevanovic[14], G Venekamp[4] and R Wartel[13]

The WISE SCIv2 Working Group - e-mail: david.kelsey@stfc.ac.uk, sci@lists.wise-community.org

Endorsement of SCI Version 2 at TNC17 (Linz)

- 1stJune 2017
- *Infrastructures endorse the governing principles and approach of SCI, as produced by WISE, as a medium of building trust between infrastructures, to facilitate the exchange of security information in the event of a cross-infrastructure incident, and the collaboration of e-Infrastructures to support the process. These Infrastructures welcome the development of an information security community for the Infrastructures, and underline that the present activities by the research and e-Infrastructures should be continued and reinforced*
- Endorsements have been received from the following infrastructures: EGI, EUDAT, GEANT, GridPP, MYREN, PRACE, SURF, WLCG, XSEDE, HBP
- https://www.geant.org/News_and_Events/Pages/supporting-security-for-collaborating-infrastructures.aspx

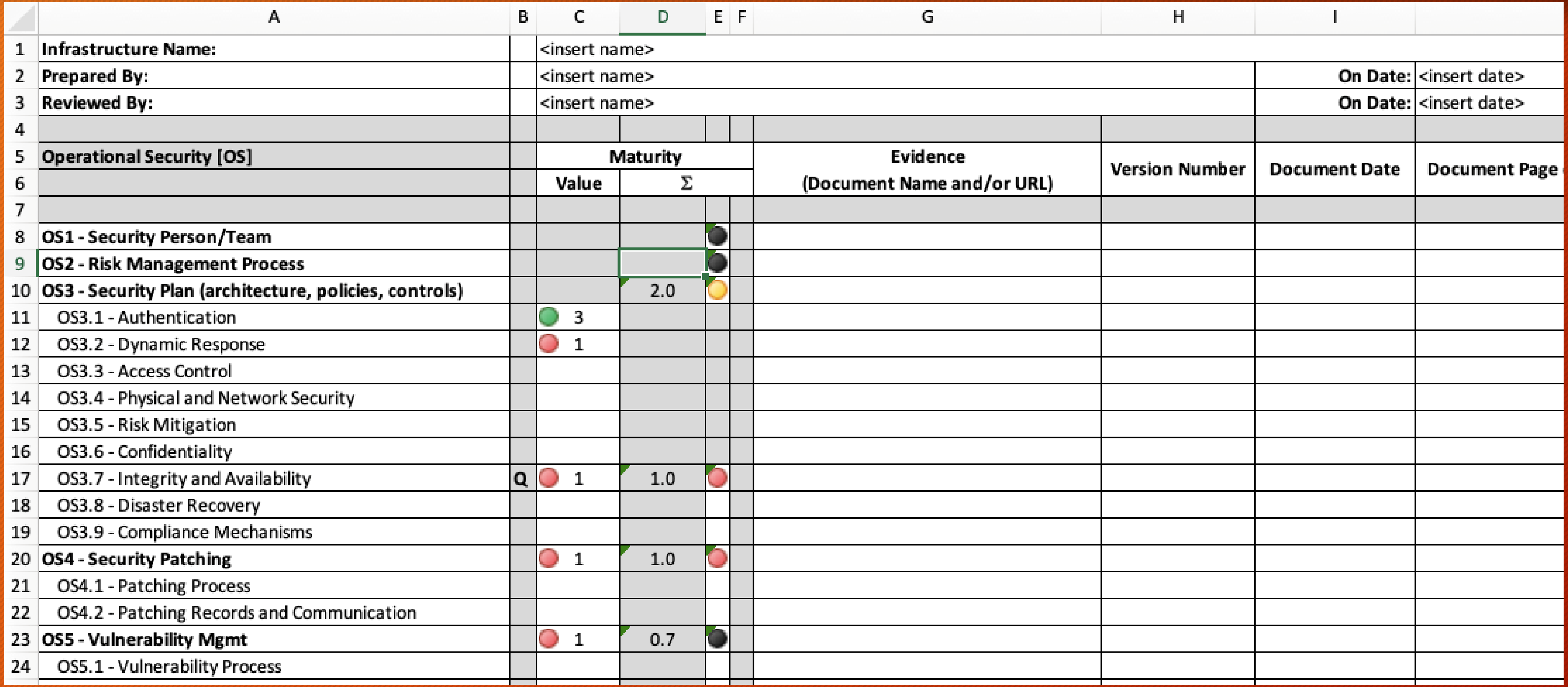
SCI requirements

- The document defined a series of numbered requirements in 5 areas
  - Operational Security
  - Incident Response
  - Traceability
  - Participant Responsibilities
  - Data protection

SCI Assessment of maturity

- To evaluate extent to which requirements are met, we recommend Infrastructures to assess the maturity of their implementations
- According to following levels:
  - Level 0: Function/feature not implemented
  - Level 1: Function/feature exists, is operationally implemented but not documented
  - Level 2: … and comprehensively documented
  - Level 3: … and reviewed by independent external body

Assessment spreadsheet



	A	B	C	D	E	F	G	H	I	
1	**Infrastructure Name:**		<insert name>							
2	**Prepared By:**		<insert name>						**On Date:**	<insert date>
3	**Reviewed By:**		<insert name>						**On Date:**	<insert date>
4										
5	**Operational Security [OS]**		**Maturity**				**Evidence**	**Version Number**	**Document Date**	**Document Page**
6			**Value**	**Σ**			**(Document Name and/or URL)**			
7										
8	**OS1 - Security Person/Team**				⚫					
9	**OS2 - Risk Management Process**				⚫					
10	**OS3 - Security Plan (architecture, policies, controls)**			2.0	🟡					
11	OS3.1 - Authentication		🟢 3							
12	OS3.2 - Dynamic Response		🔴 1							
13	OS3.3 - Access Control									
14	OS3.4 - Physical and Network Security									
15	OS3.5 - Risk Mitigation									
16	OS3.6 - Confidentiality									
17	OS3.7 - Integrity and Availability	Q	🔴 1	1.0	🔴					
18	OS3.8 - Disaster Recovery									
19	OS3.9 - Compliance Mechanisms									
20	**OS4 - Security Patching**		🔴 1	1.0	🔴					
21	OS4.1 - Patching Process									
22	OS4.2 - Patching Records and Communication									
23	**OS5 - Vulnerability Mgmt**		🔴 1	0.7	⚫					
24	OS5.1 - Vulnerability Process									

- https://wiki.geant.org/download/attachments/58131190/SCIv2-Assessment-Chart_V2-US.xlsx?version=1&modificationDate=1554550759208&api=v2

Current SCI activities

- Produce FAQ/Guidelines & Training – how to satisfy SCI V2?
- Maturity Assessments from a number of Infrastructures
  - Work already started
- WISE Baseline AUP v1.0.1 (published)
  - https://wiki.geant.org/download/attachments/123765566/WISE-SCI-Baseline-AUP-V1.0.1-draft.pdf
- Join work on improving Policy Development KIT, application to other projects
- SCI assessment –infrastructure to self-assess and peer review (e.g. in conjunction with the IGTF)
- Coherency of security policy development for collaborating infras