Wise Information Security for collaborating e-Infrastructures

WISE SCI-WG meeting

Ian Neilson, Dave Kelsey(STFC-RAL)
Uros Stevanovic (KIT)

25 May 2021

In collaboration with and
co-supported by EU H2020 EOSC-HUB & GN4-3

https://wise-community.org

SCI Version 2 – published 31 May 2017

WISE COMMUNITY

A Trust Framework for Security Collaboration among Infrastructures

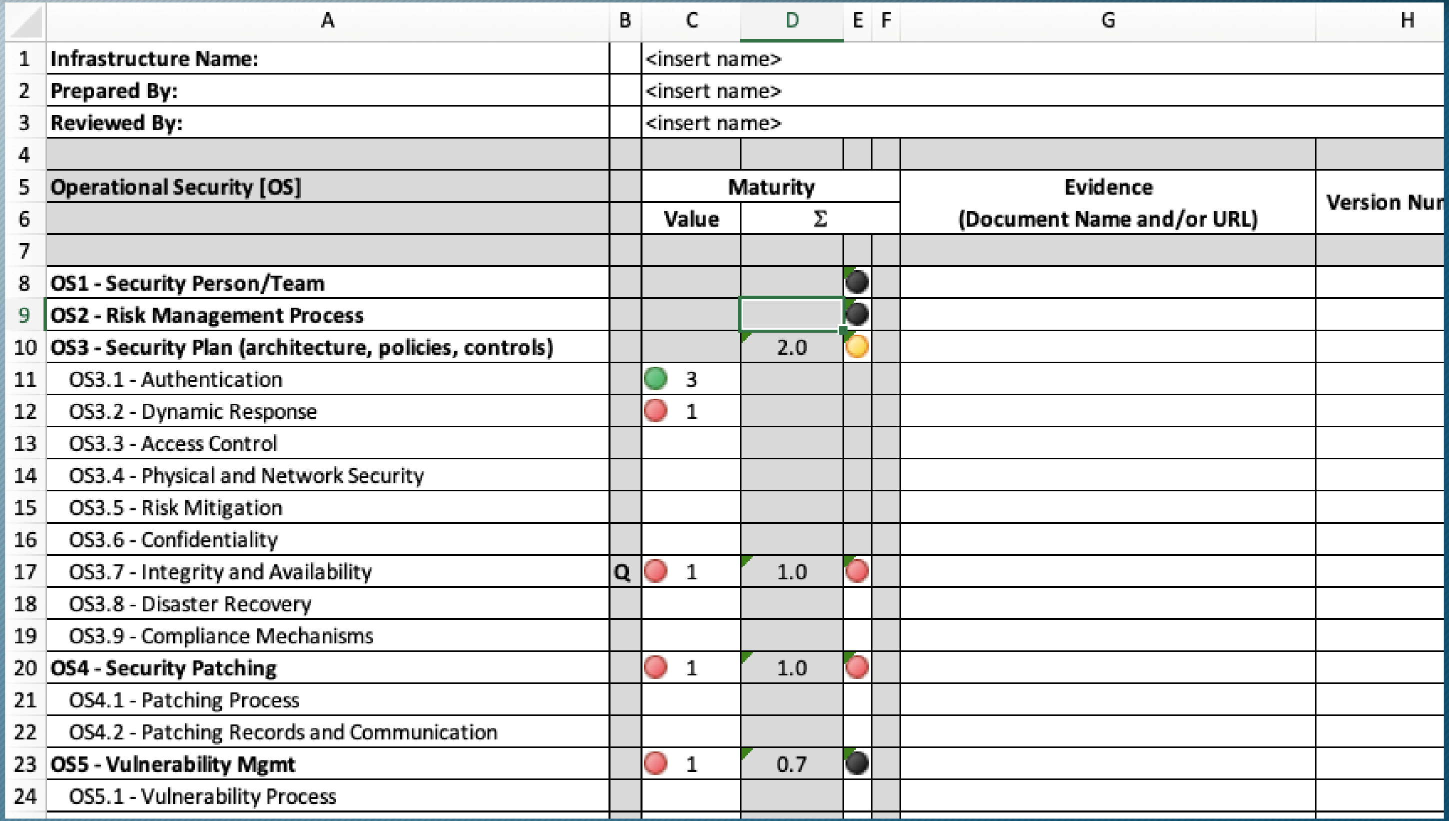
SCI version 2.0, 31 May 2017

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

- Endorsed by (all) Infrastructures (TNC17, Linz)

Assessment spreadsheet



	A	B	C	D	E	F	G	H
1	**Infrastructure Name:**		<insert name>					
2	**Prepared By:**		<insert name>					
3	**Reviewed By:**		<insert name>					
4								
5	**Operational Security [OS]**		**Maturity**				**Evidence (Document Name and/or URL)**	**Version Nur**
6			**Value**	**Σ**				
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							

- 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

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

SCI – How to implement it?

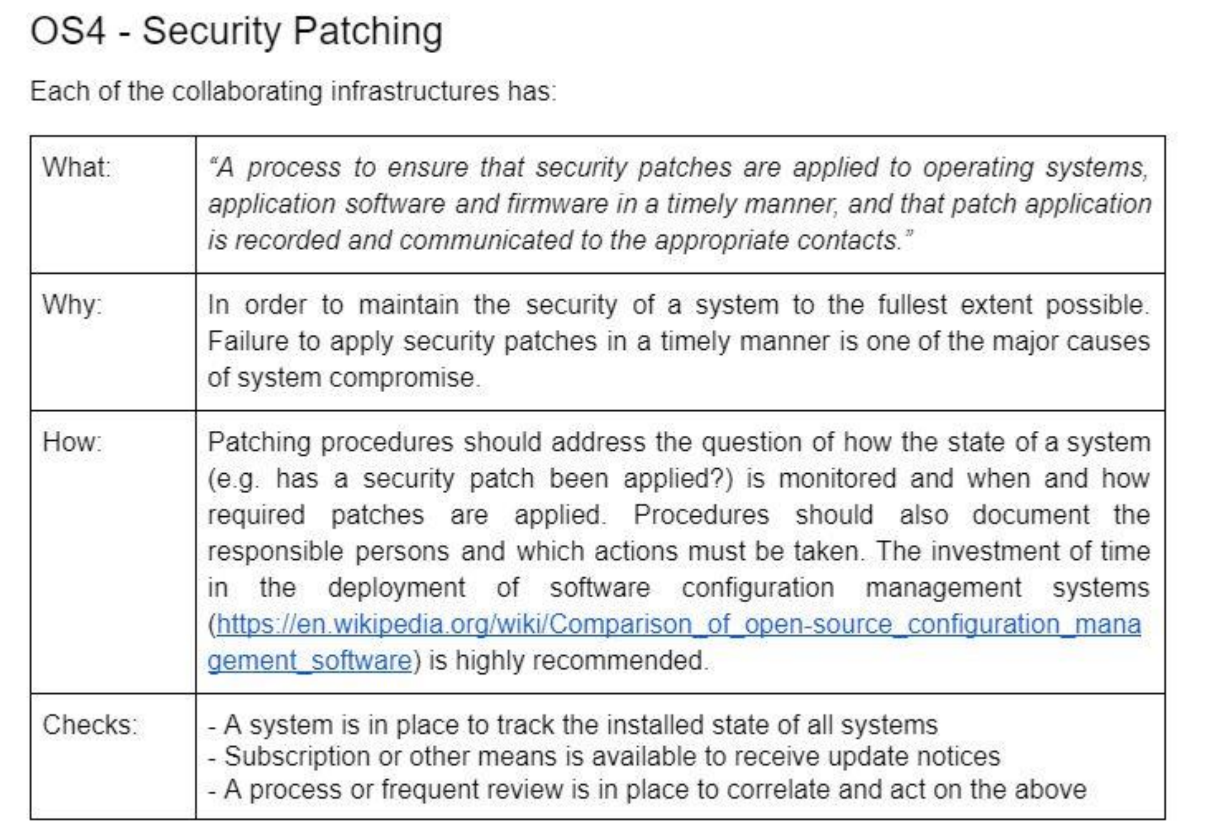
- SCI is a framework
  - Almost 30 explicit requirements
  - Sometimes not detailed or prescriptive enough
  - Different understanding of requirements
  - Requirements may vary greatly in scope and complexity
  - Some can be addressed (at least in part) by other requirements
- Guidance and explanation on implementing SCI Framework
  - How to fulfill the particular requirements
  - Checkbox steps, if possible
  - Explain the requirements, their interaction
  - Provide examples and best practices

SCI How-to

https://docs.google.com/document/d/1O2UTrKD70erpmO5DVIgn_1xpFX3NfVae_BGKPHoFuWo/edit?usp=sharing

- SCI How-to
  - What, Why, How, Checks

The guidance is intended to assist those implementing SCI and, as such, is not, primarily scoped to 'end users' - members of collections of users. Infrastructure managers, service operators, security officers, the responsibles of collections of users, and others invested in the security of an infrastructure and its services, are the intended audience.



OS4 - Security Patching

Each of the collaborating infrastructures has:

What:	*"A process to ensure that security patches are applied to operating systems, application software and firmware in a timely manner, and that patch application is recorded and communicated to the appropriate contacts."*
Why:	In order to maintain the security of a system to the fullest extent possible. Failure to apply security patches in a timely manner is one of the major causes of system compromise.
How:	Patching procedures should address the question of how the state of a system (e.g. has a security patch been applied?) is monitored and when and how required patches are applied. Procedures should also document the responsible persons and which actions must be taken. The investment of time in the deployment of software configuration management systems (https://en.wikipedia.org/wiki/Comparison_of_open-source_configuration_management_software) is highly recommended.
Checks:	- A system is in place to track the installed state of all systems - Subscription or other means is available to receive update notices - A process or frequent review is in place to correlate and act on the above

SCI How-to, status and next steps

- Initial version done
- Open the document to wider audience
- Solicit feedback!
  - & incorporate it and produce new version(s)

- Encourage Infrastructures to perform (and publish) self-assessment!