WISE SCI v2 ‘how-to’ guide

Ian Neilson, UKRI-STFC

Modified from WISE presentation 21 April 2022

A Trust Framework for Security Collaboration among Infrastructures

- https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf

3. Operational Security [OS]

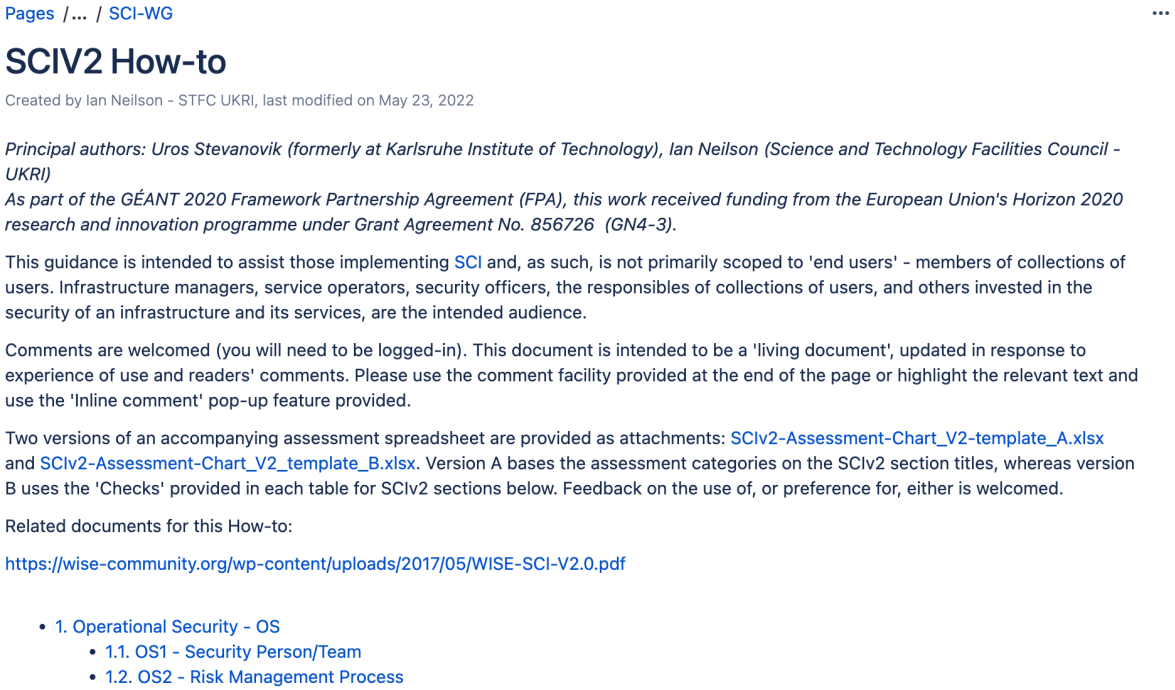
Each of the collaborating *infrastructures* has the following:

- [OS1] A person or team mandated to represent the interests of security for the *infrastructure*.
- [OS2] A process to identify and manage security risks on a regular basis.
- [OS3] A security plan (e.g., architecture, requirements, controls, policies, processes) addressing issues, such as, authentication, authorisation, access control, physical and network security, risk mitigation, confidentiality, integrity and availability, disaster recovery, together with compliance mechanisms ensuring its implementation.
- [OS4] 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.

- ❑ 29 Assertions across 5 Categories.
- ❑ How to assess the level of compliance?

Science and Technology Facilities Council

WISE words ….



Pages / ... / SCI-WG

SCIV2 How-to

Created by Ian Neilson - STFC UKRI, last modified on May 23, 2022

Principal authors: Uros Stevanovik (formerly at Karlsruhe Institute of Technology), Ian Neilson (Science and Technology Facilities Council - UKRI)
As part of the GÉANT 2020 Framework Partnership Agreement (FPA), this work received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

This 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.

Comments are welcomed (you will need to be logged-in). This document is intended to be a 'living document', updated in response to experience of use and readers' comments. Please use the comment facility provided at the end of the page or highlight the relevant text and use the 'Inline comment' pop-up feature provided.

Two versions of an accompanying assessment spreadsheet are provided as attachments: SCIv2-Assessment-Chart_V2-template_A.xlsx and SCIv2-Assessment-Chart_V2_template_B.xlsx. Version A bases the assessment categories on the SCIv2 section titles, whereas version B uses the 'Checks' provided in each table for SCIv2 sections below. Feedback on the use of, or preference for, either is welcomed.

Related documents for this How-to:

https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf

- 1. Operational Security - OS
  - 1.1. OS1 - Security Person/Team
  - 1.2. OS2 - Risk Management Process

- All information now in one place: on the WISE Wiki -
  - https://wiki.geant.org/display/WISE/SCIV2+How-to

Science and Technology Facilities Council

SCIv2 Assessment Chart (A)

- https://wiki.geant.org/download/attachments/440303650/SCIv2-Assessment-Chart_V2-template_A.xlsx?api=v2

Infrastructure Name:

	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**				**Methods of enforcement**	**Evidence (Document Name and/or URL)**
6			**Value**	**S**				
7								
8	**OS1 - Security Person/Team**		3	#REF!	REF!			
9	**OS2 - Risk Management Process**		2	#REF!	REF!			
10	**OS3 - Security Plan (architecture, policies, controls)**			2.0	2.0			
11	OS3.1 - Authentication		2					
12	OS3.2 - Dynamic Response		2					

OS3.8 - Disaster Recovery		2			
OS3.9 - Compliance Mechanisms		2			
OS4 - Security Patching		2	2.0	2.0	
OS4.1 - Patching Process		2			
OS4.2 - Patching Records and Communication		2			
OS5 - Vulnerability Mgmt		2	0.0	0.0	
OS5.1 - Vulnerability Process		2			

Science and Technology Facilities Council

SCI v2 How-To

- To provide guidance on interpreting the SCIv2 text
- *https://wiki.geant.org/display/WISE/SCIV2+How-to*

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

Science and Technology Facilities Council

SCIv2 Assessment Chart (B)

- https://wiki.geant.org/download/attachments/440303650/SCIv2-Assessment-Chart_V2_template_B.xlsx?api=v2

		Maturity			Evidence (Document Name and/or URL)
		Value	S		
Operational Security [OS]					
OS1 - Security Person/Team			**0.0**	0.0	
The person or team is appointed with clear responsibility and authority.	0	0			
Contact details for the above are published internally and externally.	0	0			
OS2 - Risk Management Process			**0.0**	0.0	
Risks and mitigations have been identified and documented.	0	0			
Reviews of the risks and mitigations take place on a regular basis.	0	0			
Actions resulting from the review are given appropriate priority and resources.	0	0			
OS3 - Security Plan (architecture, policies, controls)			**0.0**	0.0	
Documents exist defining the security requirements of the Infrastructure	0	0			

Score	Definition
Blank	Not yet assessed
0	Assessed and no implementation
1	Low implementation
2	Partial implementation
3	Full implementation
4	Full implementation with peer review

OS4 - Security Patching			**0.0**	0
A system is in place to track the installed state of all systems	0	0		
Subscription or other means is available to receive update notices	0	0		
A process or frequent review is in place to correlate and act on the above	0	0		
OS5 - Vulnerability Management			**0.0**	0

Science and Technology Facilities Council

SCI v2 Assessment options

- Need feedback for experience from use

- [OS4] 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.

A

OS3.8 - Disaster Recovery		2			
OS3.9 - Compliance Mechanisms		2			
OS4 - Security Patching		2	2.0	2.0	
OS4.1 - Patching Process		2			
OS4.2 - Patching Records and Communication		2			
OS5 - Vulnerability Mgmt		2	0.0	0.0	
OS5.1 - Vulnerability Process		2			

B

OS4 - Security Patching			**0.0**	0
A system is in place to track the installed state of all systems	0	0		
Subscription or other means is available to receive update notices	0	0		
A process or frequent review is in place to correlate and act on the above	0	0		
OS5 - Vulnerability Management			**0.0**	0

Science and Technology Facilities Council

Thank you

ian.neilson@stfc.ac.uk