Science and Technology Facilities Council

WISE COMMUNITY

WISE SCI v2 ‘how-to’ guide update

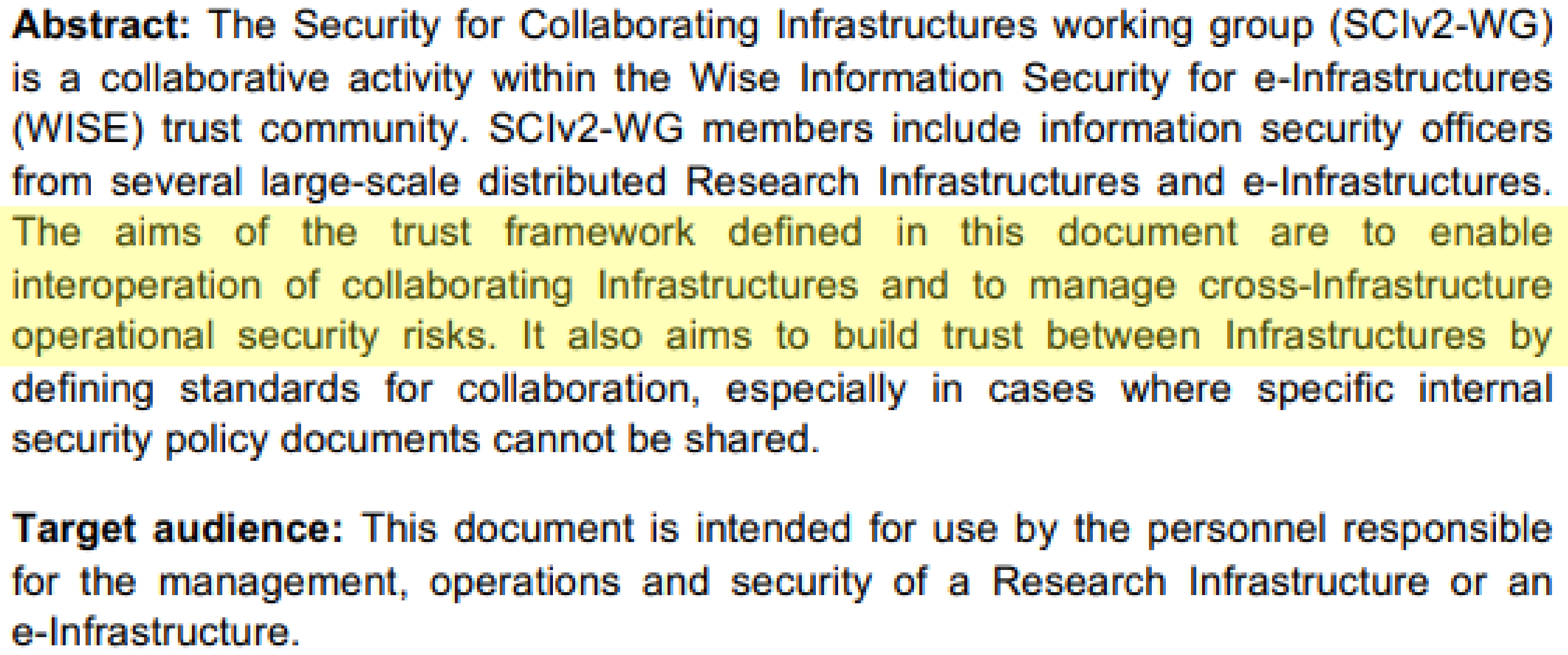
SIG-ISM - WISE Workshop, Virtual 21/04/2022

Topics

- This is an update to presentation originally from -
  - 53rd EUGridPMA meeting, Virtual, 09/2021
  - SIG-ISM - WISE Joint Workshop, Virtual, 10/2021
- Recap/context
- Progress
- “Observations”

SCI version 2.0, 31 May 2017

- “A Trust Framework for Security Collaboration among Infrastructures”

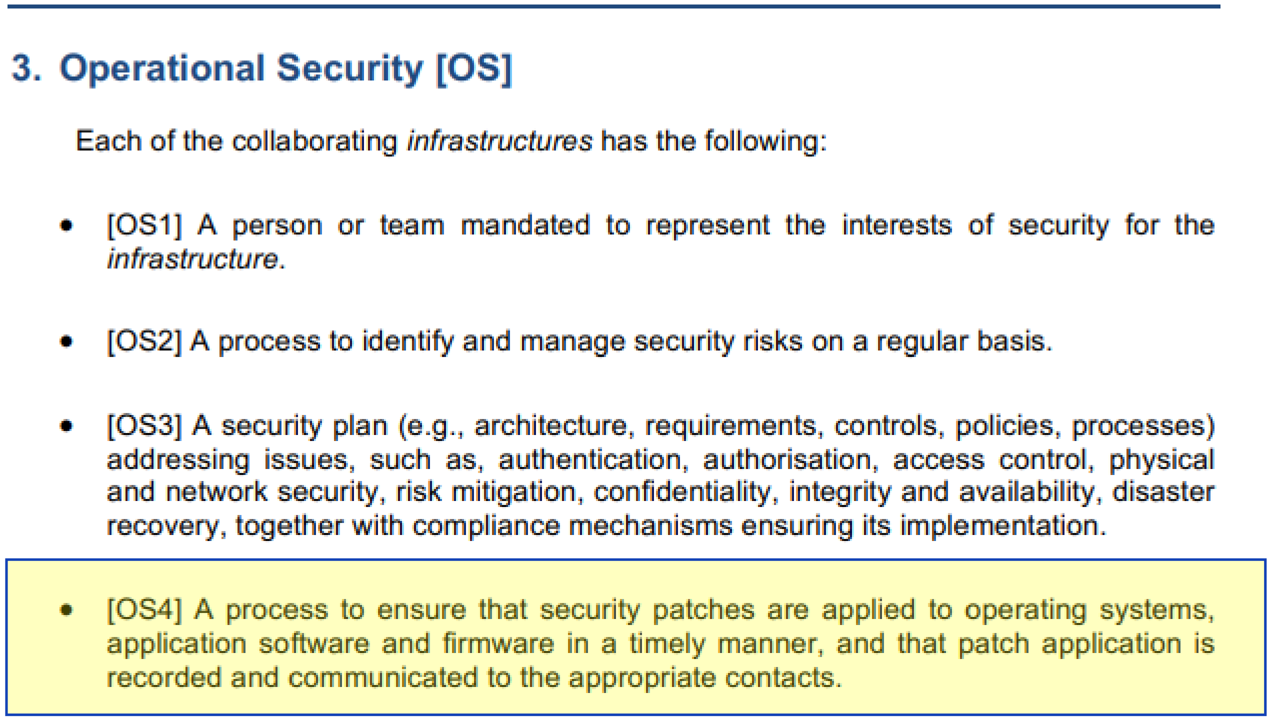


Abstract: The Security for Collaborating Infrastructures working group (SCIv2-WG) is a collaborative activity within the Wise Information Security for e-Infrastructures (WISE) trust community. SCIv2-WG members include information security officers from several large-scale distributed Research Infrastructures and e-Infrastructures. The aims of the trust framework defined in this document are to enable interoperation of collaborating Infrastructures and to manage cross-Infrastructure operational security risks. It also aims to build trust between Infrastructures by defining standards for collaboration, especially in cases where specific internal security policy documents cannot be shared.

Target audience: This document is intended for use by the personnel responsible for the management, operations and security of a Research Infrastructure or an e-Infrastructure.

A Trust Framework for Security Collaboration among Infrastructures

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



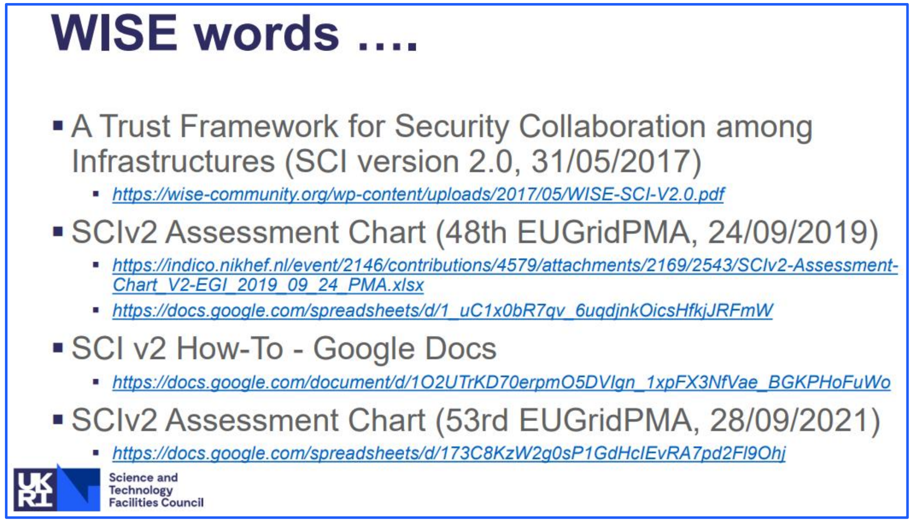
3. Operational Security [OS]

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?

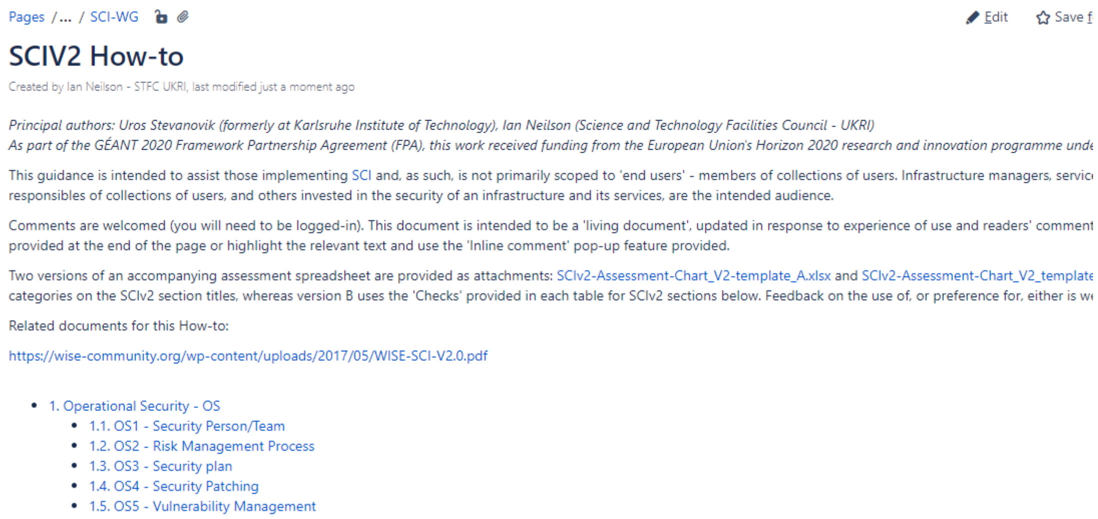
WISE words ….



WISE words ….

- A Trust Framework for Security Collaboration among Infrastructures (SCI version 2.0, 31/05/2017)
  - https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf
- SCIv2 Assessment Chart (48th EUGridPMA, 24/09/2019)
  - https://indico.nikhef.nl/event/2146/contributions/4579/attachments/2169/2543/SCIv2-Assessment-Chart_V2-EGI_2019_09_24_PMA.xlsx
  - https://docs.google.com/spreadsheets/d/1_uC1x0bR7qv_6uqdjnkOicsHfkjJRFmW
- SCI v2 How-To - Google Docs
  - https://docs.google.com/document/d/1O2UTrKD70erpmO5DVlgn_1xpFX3NfVae_BGKPHoFuWo
- SCIv2 Assessment Chart (53rd EUGridPMA, 28/09/2021)
  - https://docs.google.com/spreadsheets/d/173C8KzW2g0sP1GdHclEvRA7pd2Fl9Ohj

Science and Technology Facilities Council



SCIV2 How-to

Created by Ian Neilson - STFC UKRI, last modified just a moment ago

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 unde

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, servic
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' comment
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
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 we

Related documents for this How-to:

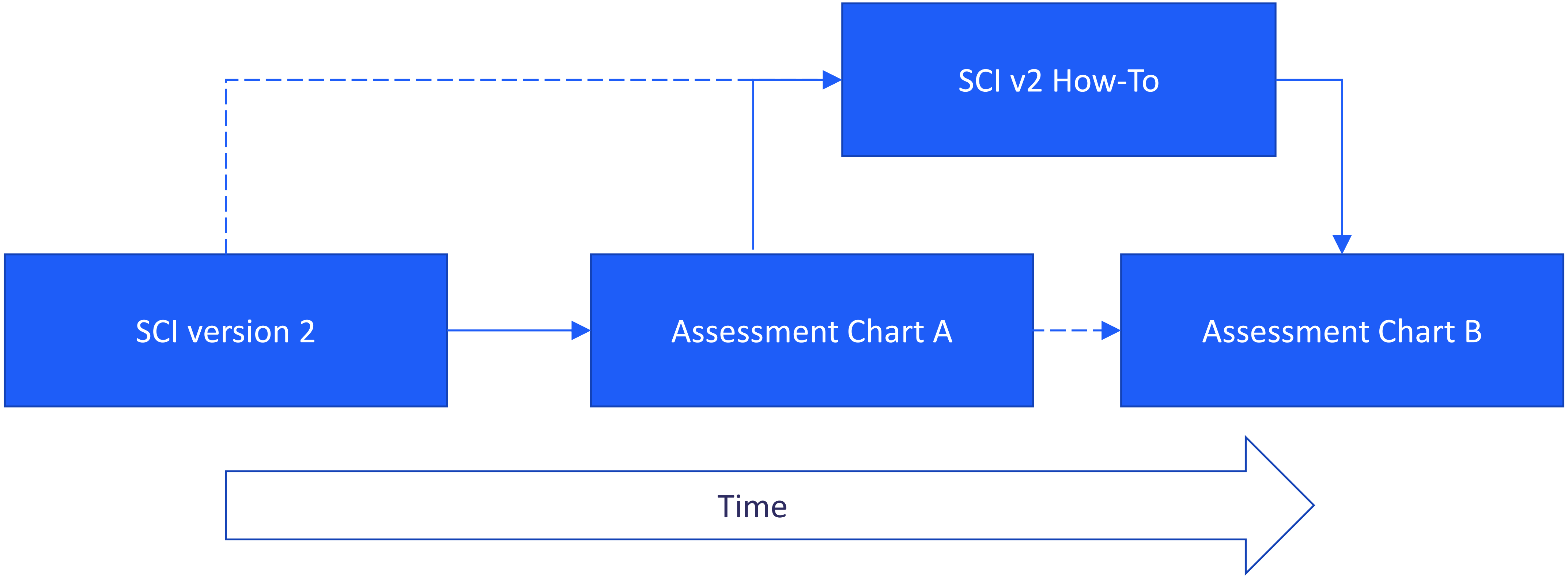
https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf

- 1. Operational Security - OS
  - 1.1. OS1 - Security Person/Team
  - 1.2. OS2 - Risk Management Process
  - 1.3. OS3 - Security plan
  - 1.4. OS4 - Security Patching
  - 1.5. OS5 - Vulnerability Management

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

Science and Technology Facilities Council

WISE pictures ….



SCI v2 How-To

SCI version 2

Assessment Chart A

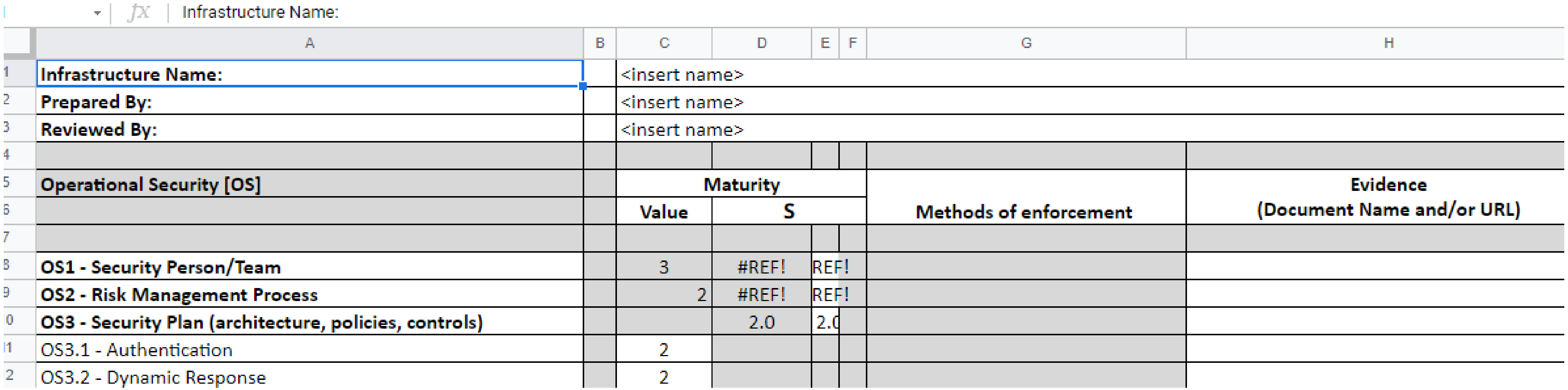
Assessment Chart B

Time

Science and Technology Facilities Council

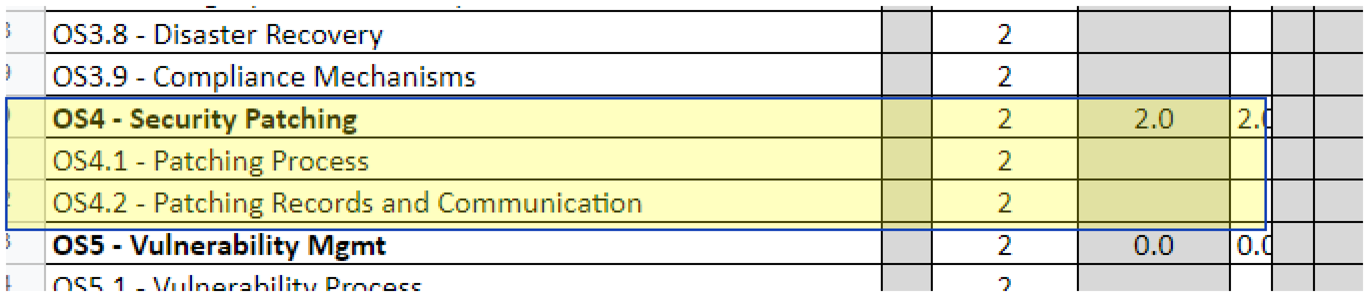
SCIv2 Assessment Chart (A)

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



fx | 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					

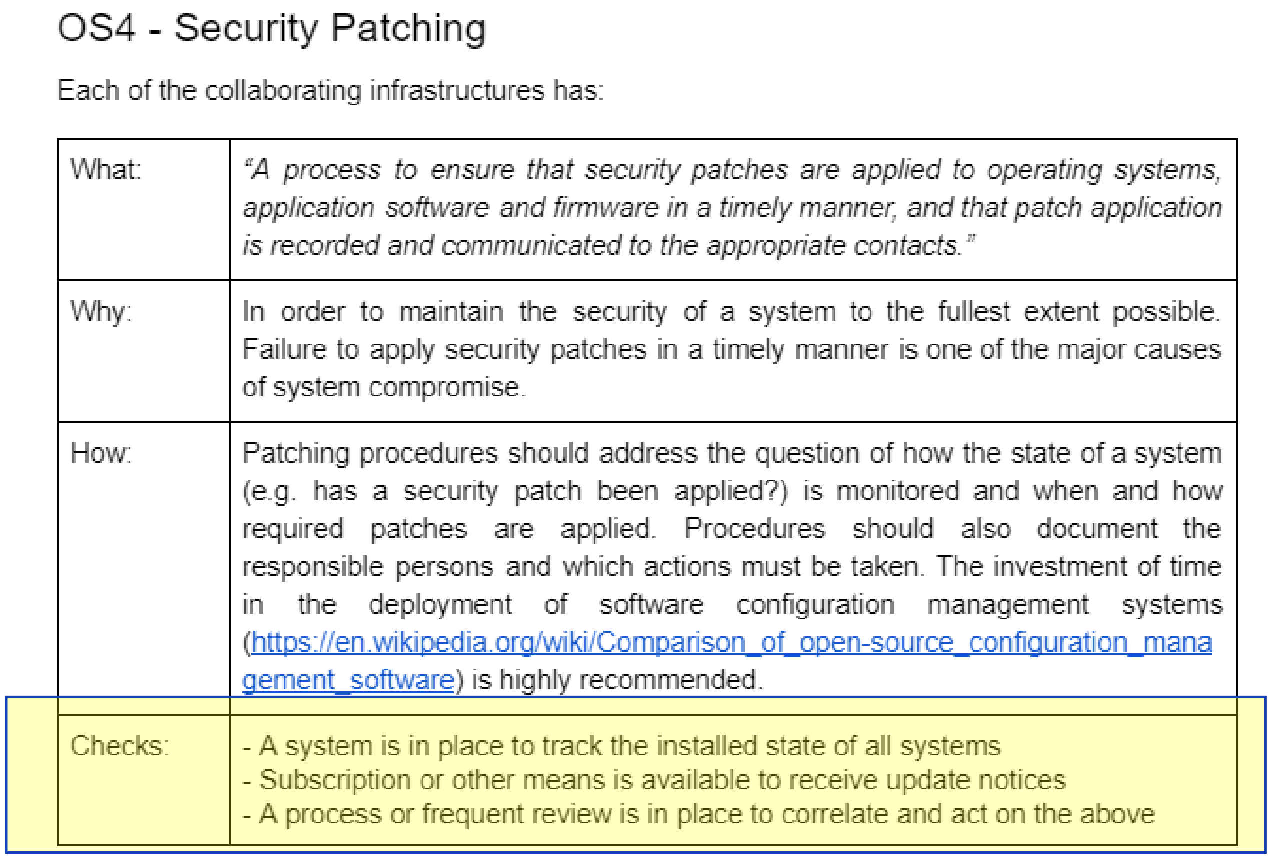


OS3.8 - Disaster Recovery		2			
OS3.9 - Compliance Mechanisms		2			
OS4 - Security Patching		2	2.0	2.0	
OS4.1 - Patching Process		2			
OS4.2 - Patching Records and Communication		2			
OS5 - Vulnerability Mgmt		2	0.0	0.0	
OS5.1 - Vulnerability Process		2			

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*



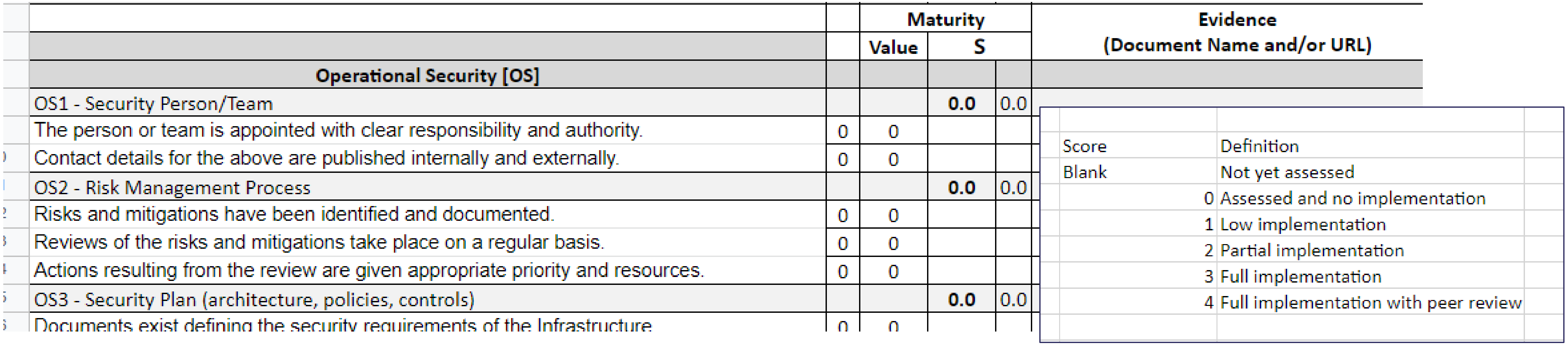
OS4 - Security Patching

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

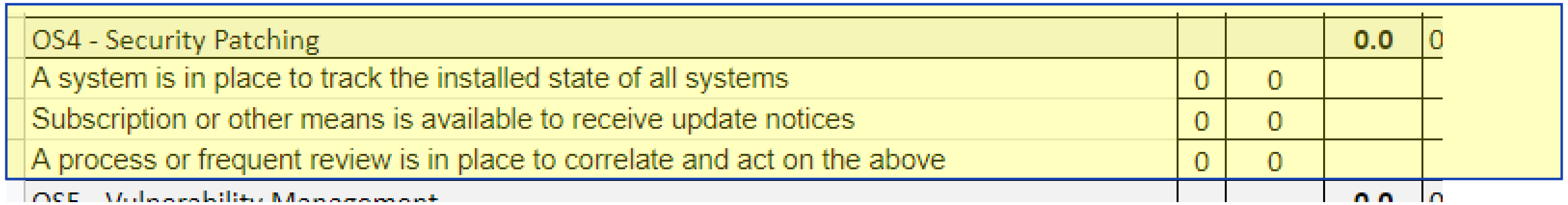
SCIv2 Assessment Chart (B)

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



		Maturity			Evidence
		Value	S		(Document Name and/or URL)
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

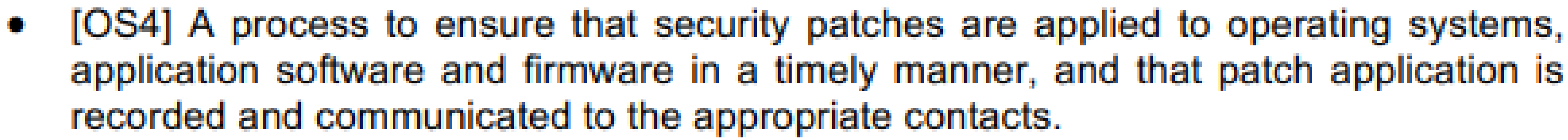


OS4 - Security Patching			0.0	0
A system is in place to track the installed state of all systems	0	0		
Subscription or other means is available to receive update notices	0	0		
A process or frequent review is in place to correlate and act on the above	0	0		
OS5 - Vulnerability Management			0.0	0

Science and Technology Facilities Council

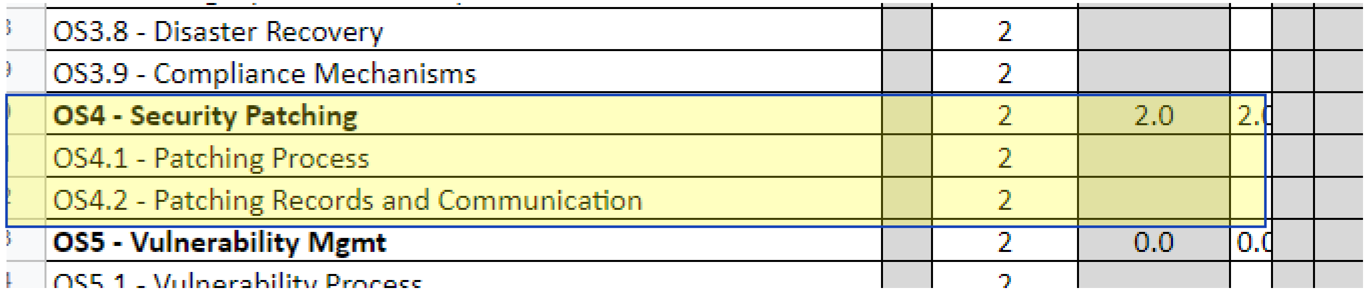
SCI v2 Assessment options

- Need feedback for experience from use



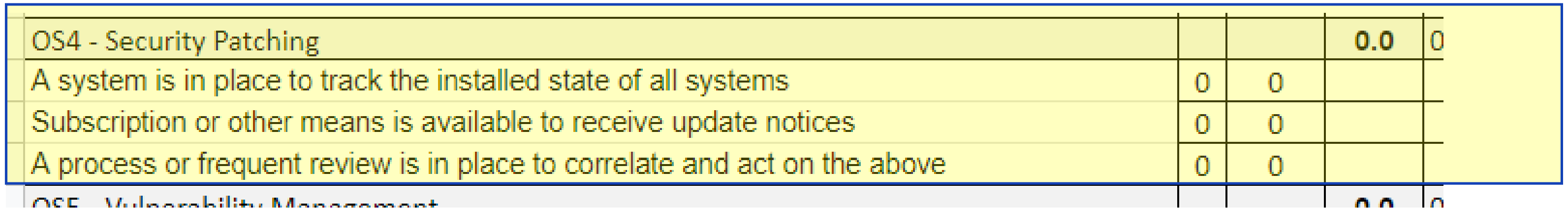
- [OS4] A process to ensure that security patches are applied to operating systems, application software and firmware in a timely manner, and that patch application is recorded and communicated to the appropriate contacts.

A



OS3.8 - Disaster Recovery		2			
OS3.9 - Compliance Mechanisms		2			
OS4 - Security Patching		2	2.0	2.	
OS4.1 - Patching Process		2			
OS4.2 - Patching Records and Communication		2			
OS5 - Vulnerability Mgmt		2	0.0	0.	
OS5.1 - Vulnerability Process		2			

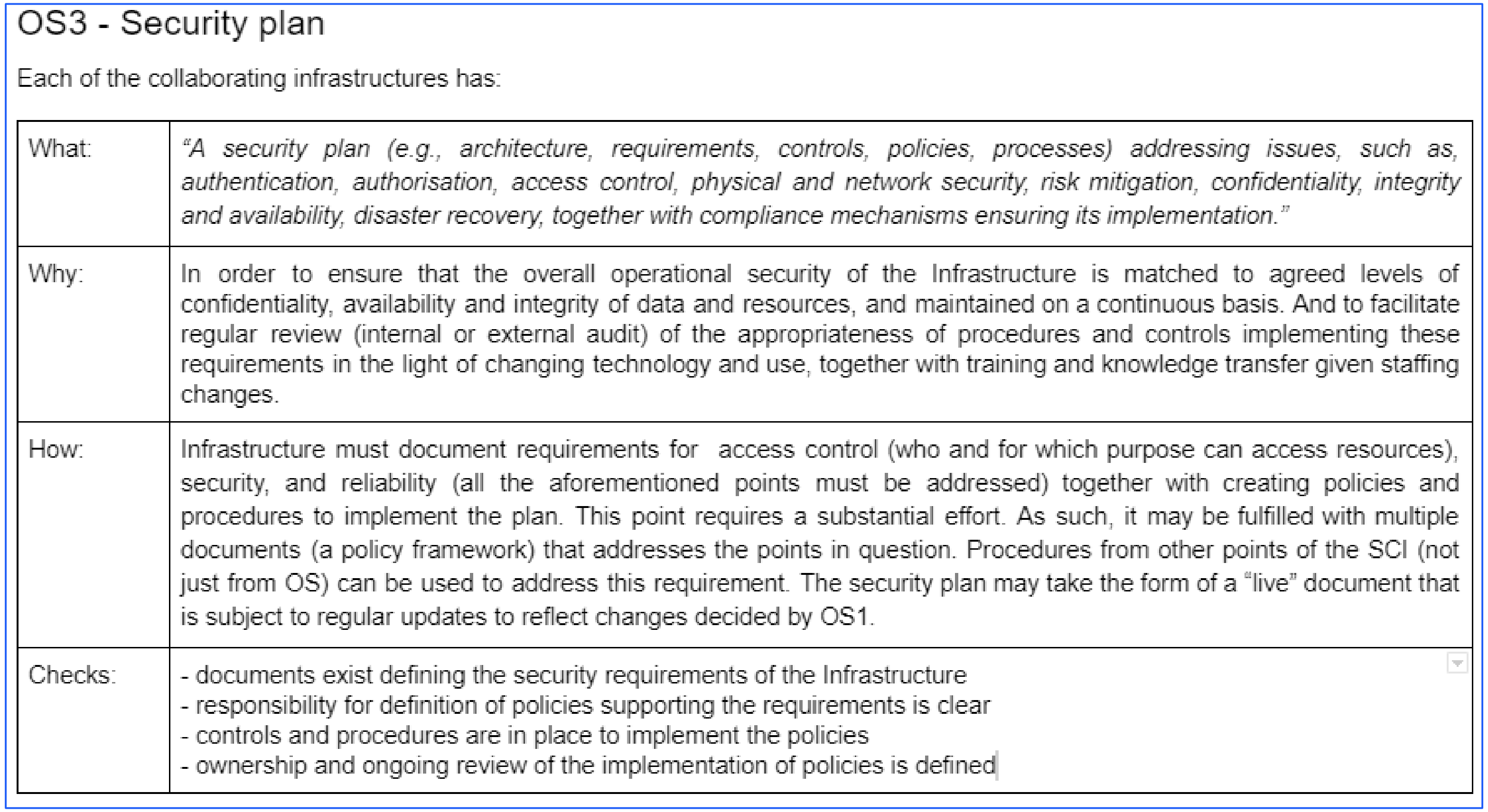
B



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

OS3 Security Plan “question”

- Very broad category requirements – hard to frame assessment.
- Text and checks included, but probably a topic for SCIv3



OS3 - Security plan

Each of the collaborating infrastructures has:

What:	*“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.”*
Why:	In order to ensure that the overall operational security of the Infrastructure is matched to agreed levels of confidentiality, availability and integrity of data and resources, and maintained on a continuous basis. And to facilitate regular review (internal or external audit) of the appropriateness of procedures and controls implementing these requirements in the light of changing technology and use, together with training and knowledge transfer given staffing changes.
How:	Infrastructure must document requirements for access control (who and for which purpose can access resources), security, and reliability (all the aforementioned points must be addressed) together with creating policies and procedures to implement the plan. This point requires a substantial effort. As such, it may be fulfilled with multiple documents (a policy framework) that addresses the points in question. Procedures from other points of the SCI (not just from OS) can be used to address this requirement. The security plan may take the form of a “live” document that is subject to regular updates to reflect changes decided by OS1.
Checks:	- documents exist defining the security requirements of the Infrastructure - responsibility for definition of policies supporting the requirements is clear - controls and procedures are in place to implement the policies - ownership and ongoing review of the implementation of policies is defined

Science and Technology Facilities Council

SCIv2 assessment in practice

- UK IRIS infrastructure use-case recently completed
  - Yet to draw firm conclusions
- Some (personal) observations and questions –
  - ‘Good in parts’ infrastructure – how to score?
    - weakest, best, average …. ?
  - Checks are definitely not standalone
    - how much do checks help?
    - IRIS assessors very familiar with SCIv2 …
  - Is yet more guidance needed on ‘score’ interpretation?
  - Requirements ‘creeping’ into the assessment
    - e.g. central logging is a scored item ….. but not mentioned in SCIv2.
  - Edits still needed
    - e.g. not useful to refer to AARC templates in the checks.

Science and
Technology
Facilities Council

Thank you

ian.neilson@stfc.ac.uk