Science and Technology Facilities Council

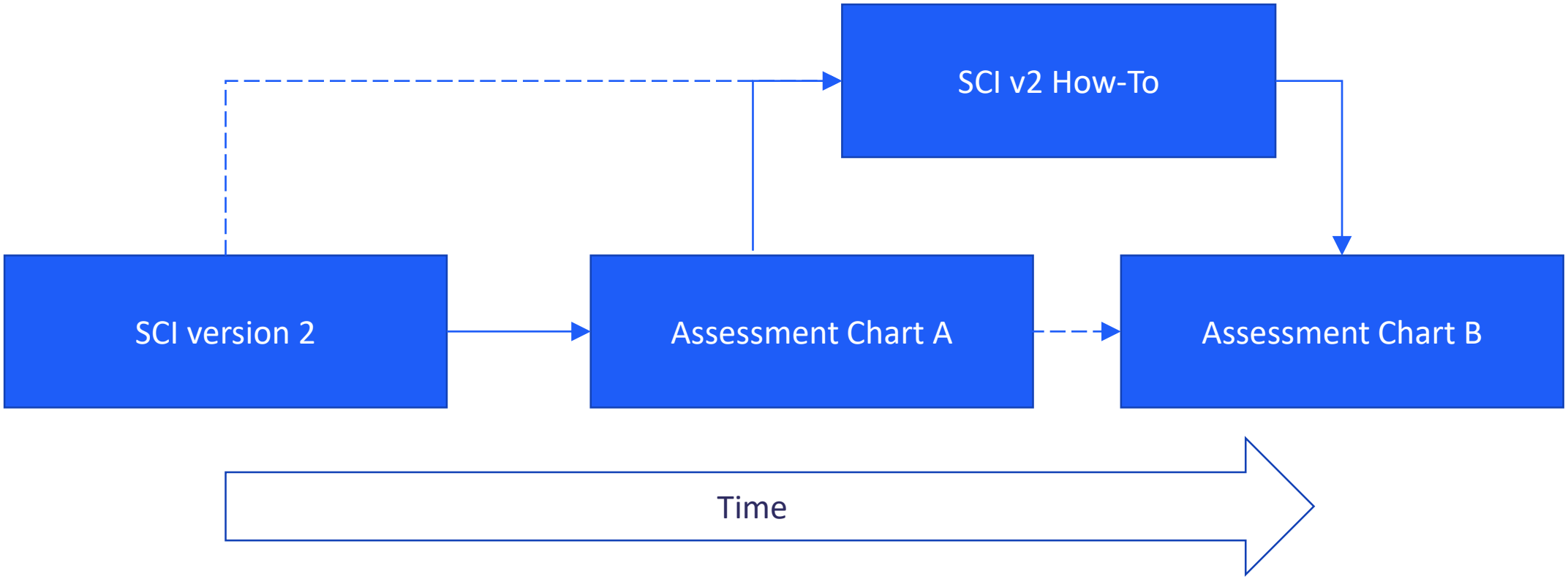
WISE SCI v2 ‘how-to’ guide development

53rd EUGridPMA meeting, Virtual, 2021

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/1O2UTrKD70erpmO5DVIgn_1xpFX3NfVae_BGKPHoFuWo*
- SCIv2 Assessment Chart (53rd EUGridPMA, 28/09/2021)
  - *https://docs.google.com/spreadsheets/d/173C8KzW2g0sP1GdHcIEvRA7pd2Fl9Ohj*

WISE pictures ….



Science and Technology Facilities Council

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:

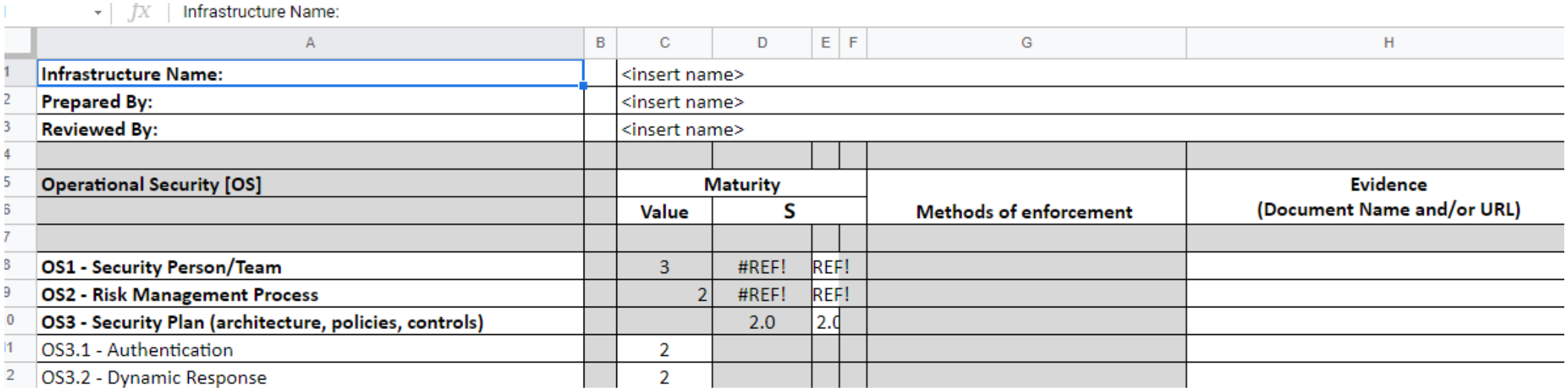
- [OS1] A person or team mandated to represent the interests of security for the *infrastructure*.
- [OS2] A process to identify and manage security risks on a regular basis.
- [OS3] A security plan (e.g., architecture, requirements, controls, policies, processes) addressing issues, such as, authentication, 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?

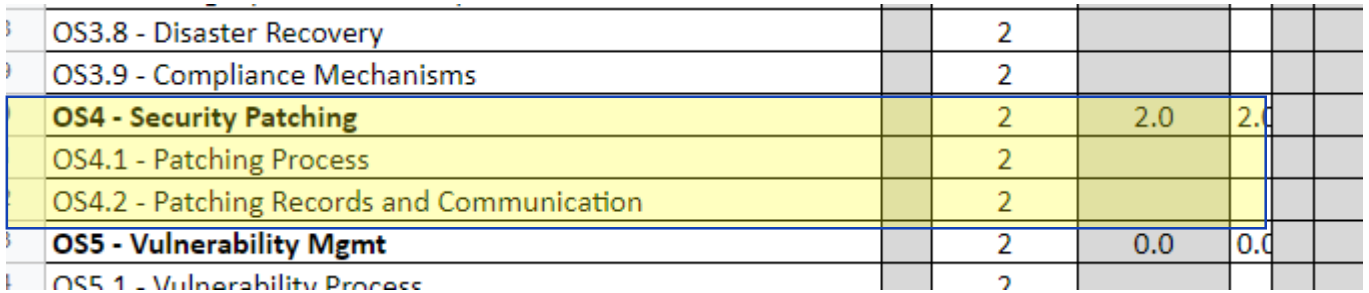
Science and Technology Facilities Council

SCIv2 Assessment Chart (A)

- https://docs.google.com/spreadsheets/d/1_uC1x0bR7qv_6uqdjnkOicsHfkjJRFmW



	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://docs.google.com/document/d/1O2UTrKD70erpmO5DVIgn_1xpFX3NfVae_BGKPHoFuWo*

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://docs.google.com/spreadsheets/d/173C8KzW2g0sP1GdHcIEvRA7pd2Fl9Ohj

			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			

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

SCI v2 How-To – “the question of OS3”

- https://docs.google.com/document/d/1O2UTrKD70erpmO5DVlgn_1xpFX3NfVae_BGKPHoFuWo
- OS3 – Security Plan
  - No clear agreement of what guidance should attach to this
  - *“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.”*
- Text added but needs community review

Science and Technology Facilities Council

SCI v2 How-To – “the question of OS3”

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

Science and Technology Facilities Council

Thank you

ian.neilson@stfc.ac.uk