Wise Information Security for collaborating e-Infrastructures

WISE SCI-WG meeting

David Kelsey (STFC-RAL, UK Research and Innovation)

10 May 2021

WISE
COMMUNITY

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

https://wise-community.org

SCI-WG – return to work! (after COVID-19)

- Last in-person WISE was in Oct 2019 - Several ongoing activities of relevance to *Security for Collaborating Infrastructures* (SCI)
  - Taking place within projects/Infrastructures (GN4-3, SLATE, IRIS, EOSC, ELIXIR, EGI …)
  - But not in the WISE WG
- Time to consult more widely and return the activity to WISE
  - For WISE "best practice" & "publications"
- Next WISE general meeting (joint with SIG-ISM)
  - Zoom on Tuesday 25th May 2021
  - https://wise-community.org/events/
- Today - plan for SCI-WG activities during this year (starting in June 2021)

Reminder - WISE Community meetings 2020

- Both held jointly with GEANT SIG-ISM (via Zoom)
  - 21-23 April 2020
  - 26 and 29 Oct 2020
- Work on SCI-related topics was presented
- And see my recent “WISE” talk at ISGC2021 *https://indico4.twgrid.org/indico/event/14/session/15/contribution/23*

Other WISE Working Groups

Current Working Groups

- **Trust and policy issues related to the Security for Collaborating Infrastructures trust framework (SCI-WG)**
- Security Communications Challenge Coordination Working Group (SCCC-JWG) – joint with SIG-ISM
- Incident Response & Threat Intelligence Working Group (IRTI-WG)
- Risk Assessment WISE (RAW-WG) – joint with SIG-ISM

Still being considered (as proposed at last WISE meeting)

- Best Practices for handling Software Vulnerabilities

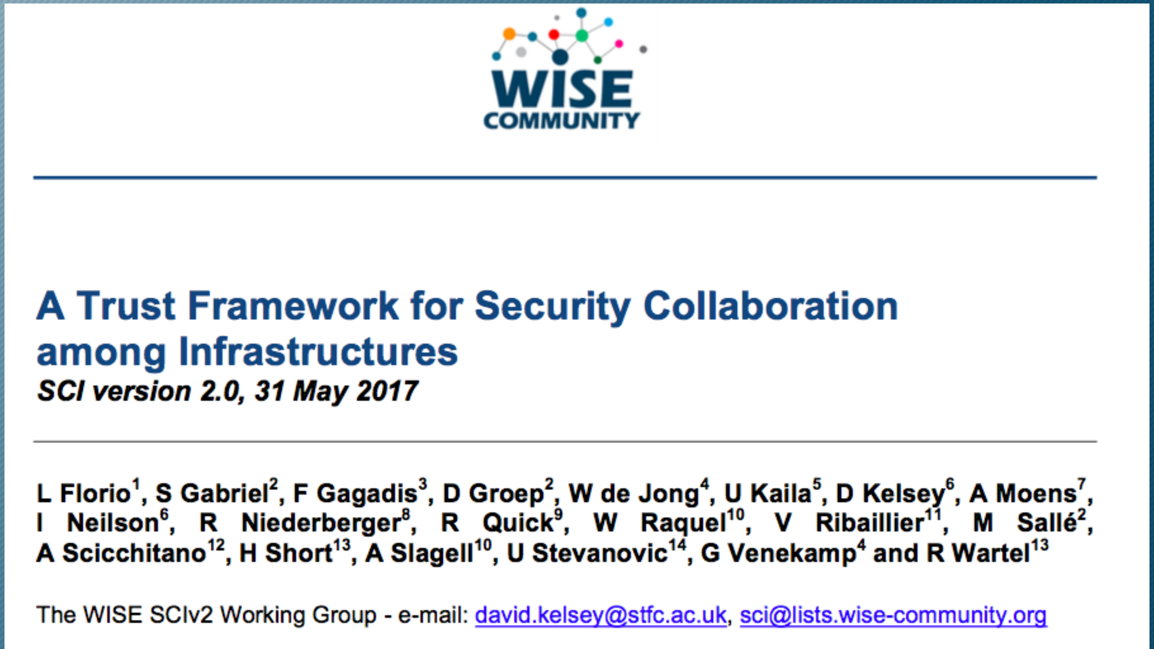
WISE/SCI in 2021 (presented Oct 2020 WISE)

- SCI-WG
  - Complete the HowTo Guidance on maturity assessment
    - & encourage Infrastructures to perform self-assessment
  - Include feedback from USA SLATE policy work
    - Does this mean SCI version 3?
  - Produce updated policy templates from AARC PDK

SCI-WG - Shared threats & shared users

- Infrastructures are subject to many of the same threats
  - Shared technology, middleware, applications and users
- User communities use multiple e-Infrastructures
  - Often using same federated identity credentials
- Security incidents often spread by following the user
  - E.g. compromised credentials
- e-Infrastructure security teams need to collaborate

SCI Version 2 – published 31 May 2017



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)

- 1st June 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

Now – consider work for SCI-WG

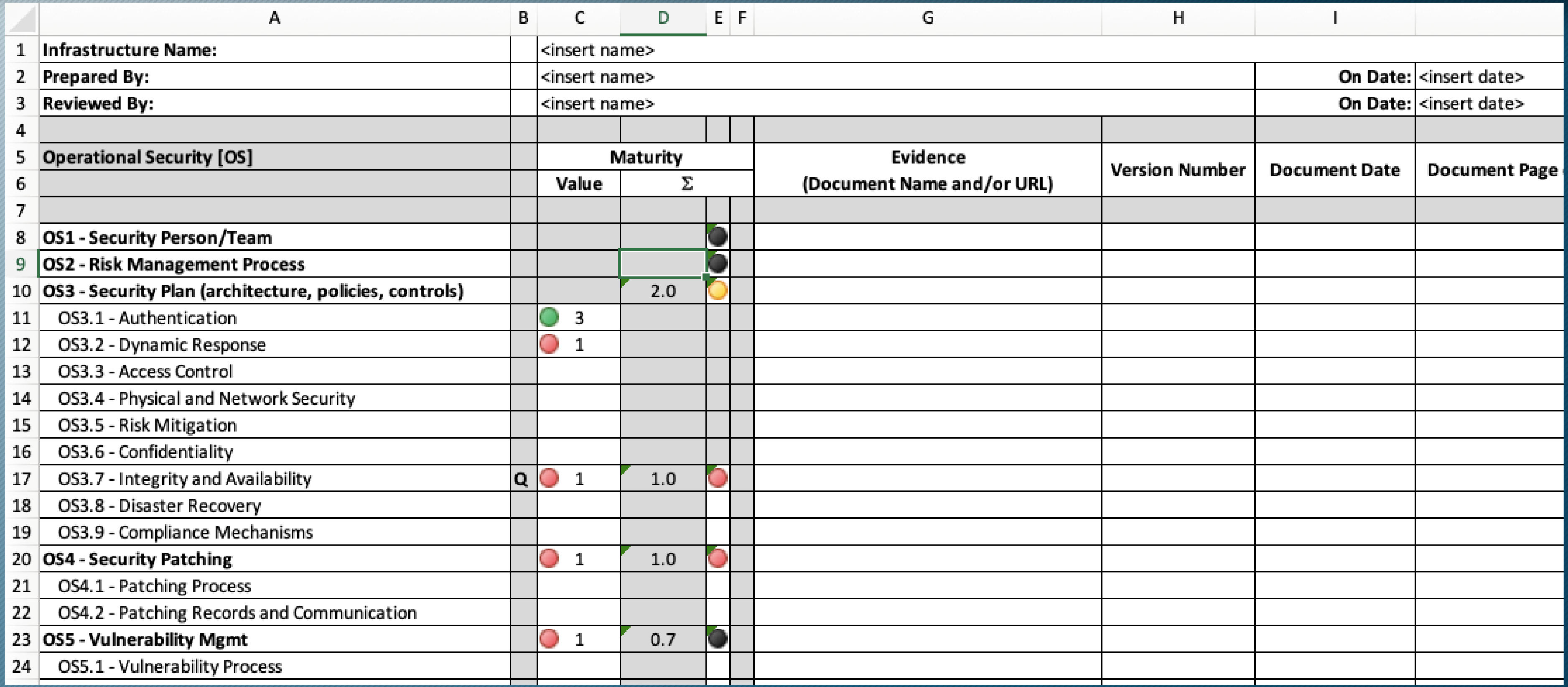
As more than one activity:

- Do we have just one set of meetings and tackle topics sequentially?
  - If so, which do we do first?
- Or do we create sub-task meetings and tackle in parallel?

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									

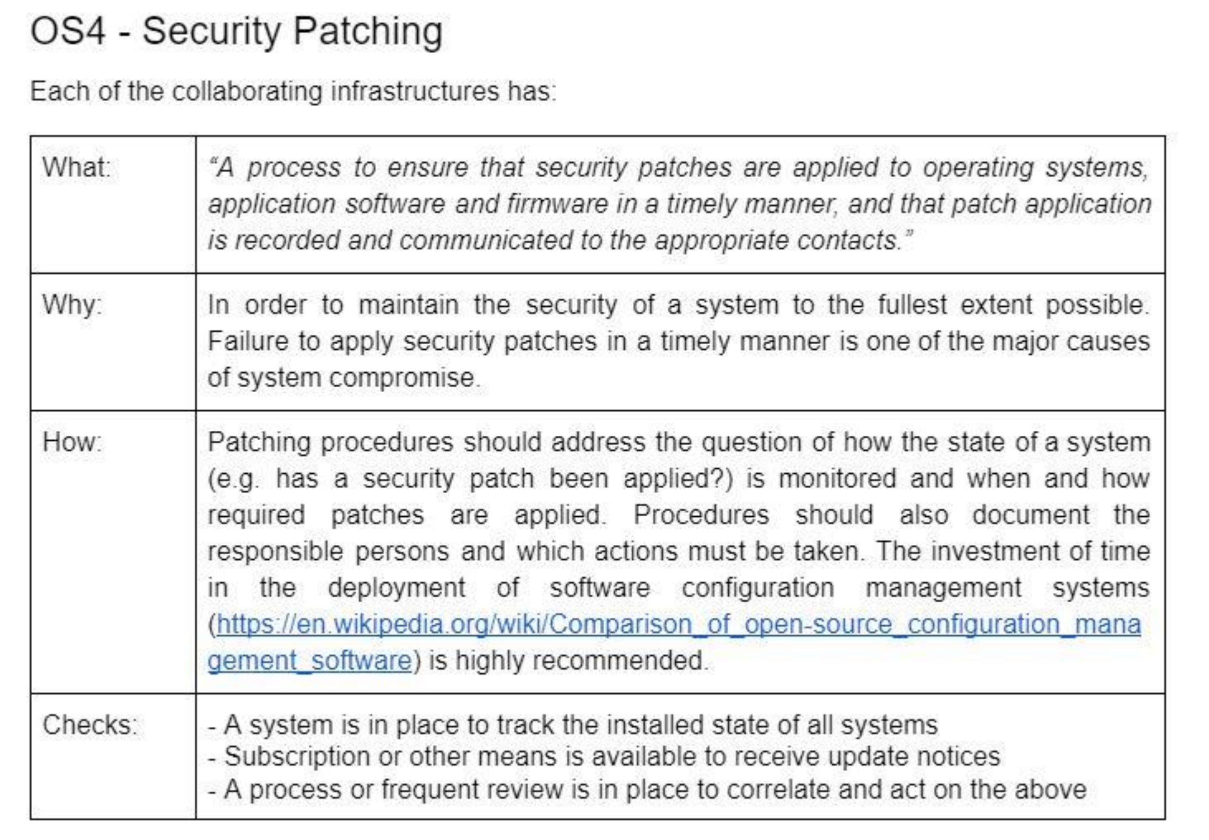
- https://wiki.geant.org/download/attachments/58131190/SCIv2-Assessment-Chart_V2-US.xlsx?version=1&modificationDate=1554550759208&api=v2

SCI How-to?

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

- SCI is a framework
  - Sometimes not detailed or prescriptive enough
  - Different understanding of requirements
  - Requirements may vary greatly in scope and complexity

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

SLATE policies and procedures

- WISE meeting in Oct 2020: Tom Barton showed how application container security isn't really addressed in SCI v2
- Worked with SLATE team to devise procedures to review containers submitted for inclusion in SLATE's stable catalog
- New application review procedures are initially complete and they are looking for critical feedback
- There's been some circulation among OSG and ESnet security people
- What about asking the WISE/SCI community for feedback?
- And should an SCI v3 be developed to include some of this?

- The materials are available:

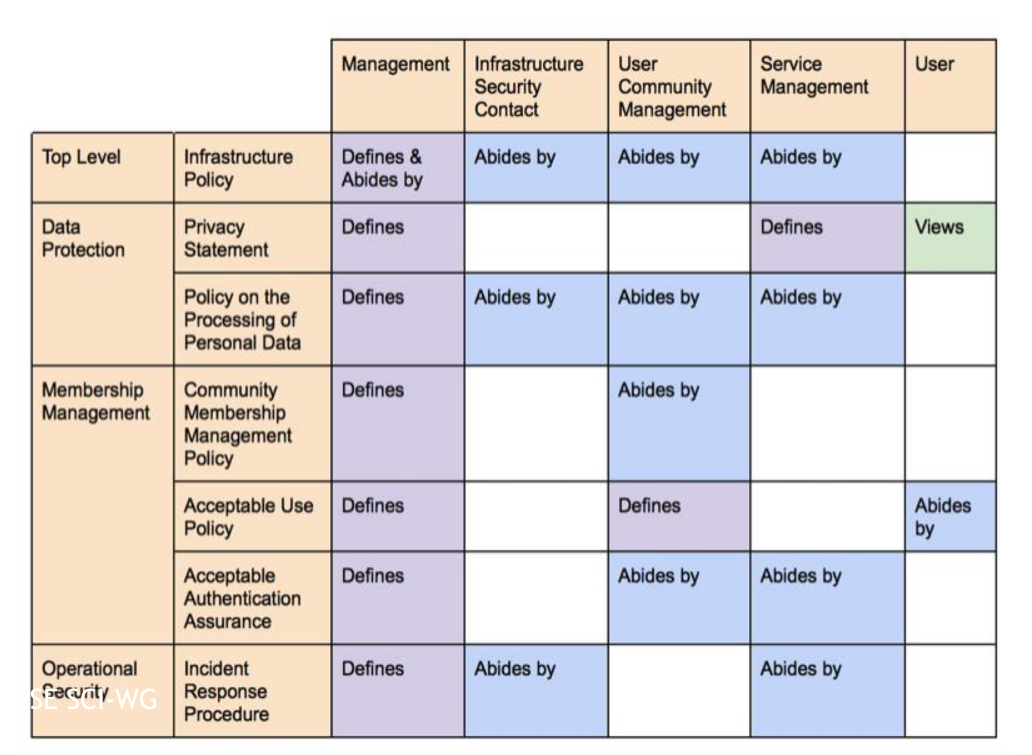
1. SLATE Application Development and Review Procedures
2. SLATE Application Reviewer Obligations
3. SLATE Application Developer Obligations

Development of AARC PDK by WISE SCI-WG

- Involve the widest experience from many Infrastructures and policy groups
- Infrastructures using/considering the AARC PDK include
  - EOSC-hub, IRIS(UK), EGI, ELIXIR, WLCG, SLATE(USA)
- Policy templates are useful to new Infrastructures and help build trust and interoperability (compliant with SCI Trust Framework)
- WISE SCI will collect feedback from Infrastructures
  - And use this if/when a new version of a template is required
- Unlike AUP, new templates may contain optional components
  - Infrastructures just use the components that work for them

Building on AARC PDK in WISE SCI-WG

https://aarc-project.eu/policies/policy-development-kit/



		Management	Infrastructure Security Contact	User Community Management	Service Management	User
Top Level	Infrastructure Policy	Defines & Abides by	Abides by	Abides by	Abides by	
Data Protection	Privacy Statement	Defines			Defines	Views
	Policy on the Processing of Personal Data	Defines	Abides by	Abides by	Abides by	
Membership Management	Community Membership Management Policy	Defines		Abides by		
	Acceptable Use Policy	Defines		Defines		Abides by
	Acceptable Authentication Assurance	Defines		Abides by	Abides by	
Operational Security	Incident Response Procedure	Defines	Abides by		Abides by	

Policy Area	New Template	Lead Participants
Top Level	Infrastructure Policy	IRIS (UK), EOSC-hub
Data Protection	Privacy Statement	WLCG, IRIS
Data Protection	Policy on the Processing of Personal Data	EGI, WLCG
Membership	Community Policy	IRIS, EOSC, GN4-3, IGTF
Membership	Acceptable Authentication Assurance	GN4-3, IGTF
Operational Security	Incident Response	eduGAIN, Sirtfi, GN4-3, EOSC & many opsec groups
Operational Security	Service Operations	EOSC-hub, IRIS

And ELIXIR too

Which policies to work on first?

- Security of Service Operations
- Community Operations
- Top-level Security Policy
- Update the WISE Baseline AUP (a version 2)
- Data Privacy (GDPR etc)
- Identity Management/Assurance

Questions? And then discussion?

- SCI V2 – maturity assessment and “HowTo” guidance
  - What about peer review and/or external audit?
- SLATE policy – feedback from SCI
- Updates to AARC PDK
  - Which policy first?
- Any other topics? General discussion?
  - Eventually – produce updated document – SCI version 3
    - Better treatment of federations and links to eduGAIN, Assurance etc
    - Include improvements/feedback from Sirtfi, Snctfi

Next steps

- Report to the WISE meeting on 25th May 2021
- Do some work by email and commenting on documents
  - Can start now/soon
  - SCI HowTo?
  - SLATE policies/procedures
- SCI-WG meetings
  - Finalise SCI HowTo?
  - Start work on first update to AARC PDK
    - Service Operations Security Policy?
- When and how frequent? Start in June 2021. Thursdays? 16:00 CEST?
  - Proposal – One hour every two weeks at time to allow USA and EU?