Science and Technology Facilities Council

IRIS Security 2021

David Crooks
david.crooks@stfc.ac.uk

iris

Overview

- IRIS Trust Framework
- IRIS Security Maturity Report

IRIS Trust Framework status

- Policies now approved by Delivery Board
  - IRIS Infrastructure Security Policy
  - IRIS AUP
  - IRIS IAM Privacy Notice

- IRIS Security risk assessment now underway
  - Focusing on IRIS IAM and attached services
  - Focus on appropriate assurance profiles

UKRI Science and Technology Facilities Council iris

IRIS Trust Framework 2021

- Acceptable Authentication Assurance Policy
  - Codify the assurance profiles appropriate for use with IRIS services
- Community Security Policy
  - Following Service Operations Security Policy
  - Establish expectations of IRIS communities from a security standpoint

IRIS Security 2021

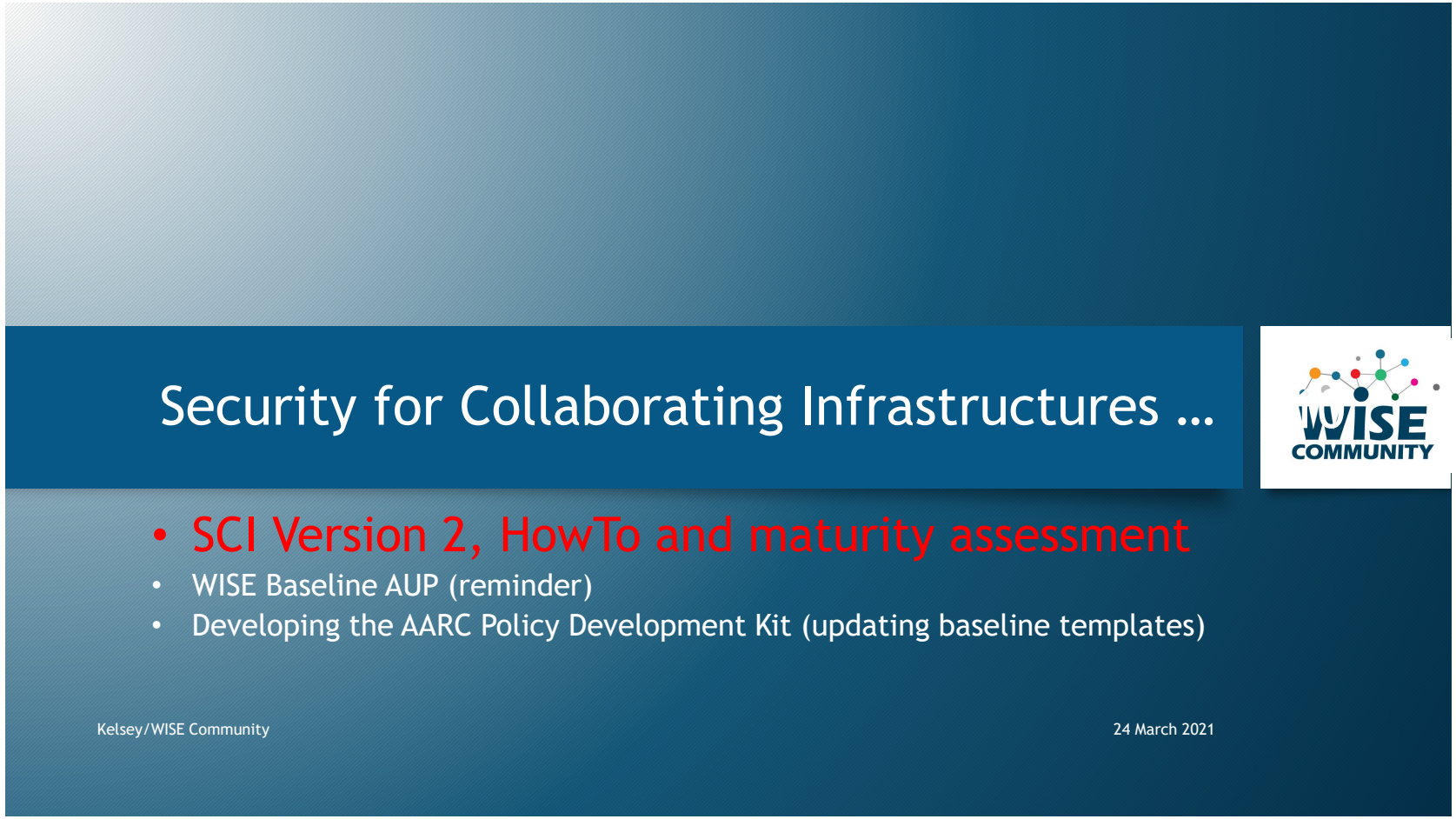
- Last year of IRIS 4x4
  - Excellent opportunity to see how we have developed
  - Inform what next steps to take

- IRIS Security Maturity Report
  - SCIv2 Framework Assessment
  - IRIS Security Roadmap

Science and Technology Facilities Council

iris

SCIv2 Framework



UKRI Science and Technology Facilities Council

iris

SCIv2 Framework

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

Science and Technology Facilities Council

iris

SCIv2 Framework

SCI requirements

- The document defined a series of numbered requirements in 5 areas
  - Operational Security
  - Incident Response
  - Traceability
  - Participant Responsibilities
  - Data protection

SCIv2 Framework

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

SCIv2 Framework

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

IRIS Security 2021

- Perform maturity assessment based on SCIv2 framework
- From this perform gap analysis to create an IRIS Security Roadmap

Science and Technology Facilities Council

iris